# Cyclic Orbit Codes

Anna-Lena Trautmann, Felice Manganiello, Michael Braun and Joachim Rosenthal

*Abstract*—In network coding a constant dimension code consists of a set of $k$-dimensional subspaces of $\mathbb{F}_q^n$. Orbit codes are constant dimension codes which are defined as orbits of a subgroup of the general linear group, acting on the set of all subspaces of $\mathbb{F}_q^n$. If the acting group is cyclic, the corresponding orbit codes are called cyclic orbit codes. In this paper we give a classification of cyclic orbit codes and propose a decoding procedure for a particular subclass of cyclic orbit codes.

*Index Terms*—Network coding, subspace codes, Grassmannian, group action, general linear group, Singer cycle .

## I. INTRODUCTION AND RELATED WORK

NETWORK coding describes a method for attaining a maximum information flow within a network, that is an acyclic directed graph with possibly several sources and sinks. The notion first arose in [1]. An algebraic approach to coding in non-coherent networks, called *random network coding*, with respect to error correction and the corresponding transmission model is given in the paper of Kötter and Kschischang [18]. There they specify under which conditions errors can be recognized and corrected.

In the random network coding setting a message corresponds to a subspace $\mathcal{V}$ of a finite $n$-dimensional vector space over a finite field $\mathbb{F}_q$, denoted by $\mathcal{V} \leq \mathbb{F}_q^n$. Generating vectors of this subspace will be injected at the sources of the network and will be transmitted to their neighboring nodes. These nodes gather some vectors, linearly combine them, and transmit these linear combinations to their neighbors. In the end the receiver nodes collect linear combinations of the original injected vectors.

In the error-free case the receiver can reconstruct the whole subspace $\mathcal{S}$ from the collected vectors.

In real world applications, networks are exposed to noise such that messages can be lost or modified during the transmission of $\mathcal{V}$. It is also possible that some node wants to disrupt the transmission flow by injecting wrong vectors. Thus, on one hand, some vectors of $\mathcal{V}$ might be lost and a smaller subspace $\mathcal{V}' < \mathcal{V}$ will be received. On the other hand, vectors which are not contained in $\mathcal{V}$ might be received. These erroneous vectors span a vector space $\mathcal{E}$, thus $\mathcal{R} = \mathcal{V}' \oplus \mathcal{E}$ will be received. Vectors lost during transmission are called *erasures* and additional received vectors not contained in $\mathcal{V}$ are called *errors*.

Since Kötter and Kschischang published their pioneering article [18] several papers about the structure of network codes appeared, e. g. [6], [8], [9], [10], [11], [17], [22], [23],

[25], [26], [29], [30]. A survey on all most important results including constructions and bounds of subspace codes which appeared before 2010 offers the paper of Khaleghi et al. [16].

In [17] Kohnert and Kurz constructed constant dimension codes by solving a Diophantine system of linear equations. In order to obtain a reduction of the huge system of equations they prescribed a group of automorphisms which is a subgroup of the general linear group. The corresponding codes are unions of orbits of that prescribed group on $k$-subspaces. This approach by prescribing a group of automorphisms and solving a Diophantine system of equations was first introduced by Kramer and Mesner [19] in 1976 for the construction of combinatorial $t$-designs.

The concept of defining codes as orbits of certain groups traces back to Slepian [27] where Euclidian spaces were considered—the corresponding codes are called *group codes*. In the network coding setting Trautmann et al. [29] defined such codes as *orbit codes*. The applied groups are again subgroups of the general linear group. If the acting group is the Singer cycle group Elsenhans et al. [8] gave a decoding algorithm for constant 3-dimensional orbit codes. A subclass of orbit codes define the cyclic subgroups of the general linear groups, the corresponding orbit codes are called *cyclic orbit codes*—they were introduced by Trautmann and Rosenthal in [30], where the authors started with a partial characterization of these cyclic orbit codes.

The goal of this paper is to continue the work of [30]. We describe cyclic orbit codes, give a complete characterization of these codes and propose a decoding algorithm for irreducible cyclic orbit codes which is different from the approach introduced in [8].

The paper is organized as follows: In the second section we give the major preliminaries and consider some different point of views on subspace codes.

In the third section we motivate and describe orbit codes in a general setting by considering group actions on metric sets. Furthermore, we give an interpretation of maximum likelihood decoding in terms of the group actions.

In Section IV we classify cyclic orbit codes. For each type given by the conjugacy class of cyclic subgroups of the general linear group we characterize the corresponding cyclic orbit codes. Section V deals with their size and the minimum distance.

In Section VI we investigate a decoding algorithm for cyclic orbit codes arising from Singer cycles. We compare the complexity of this algorithm with different decoding procedures already proposed for other types of constant dimension codes.

Finally we conclude with the summary of the main results of this paper, give some suggestions for further research, and gather some open questions.

## II. BACKGROUND

Let $\mathbb{F}_q$ be the finite field with $q$ elements (where $q$ is a prime power) and let $n$ be natural number.

When $\mathcal{U}$ is a subspace of the vector space $\mathbb{F}_q^n$ we will use the notation $\mathcal{U} \leq \mathbb{F}_q^n$. The dimension will be abbreviated by $\dim(\mathcal{U})$. The set of all subspaces of $\mathbb{F}_q^n$ of dimension $k$ is called *Grassmann variety* or simply *Grassmannian* and is denoted by

$$\mathcal{G}_q(k,n) := \{\mathcal{U} \leq \mathbb{F}_q^n \mid \dim(\mathcal{U}) = k\}.$$

The cardinality of this set is given by the *q-Binomial coefficient*, also called *Gaussian number*,

$$|\mathcal{G}_q(k,n)| = \begin{bmatrix} n \\ k \end{bmatrix}_q := \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}.$$

The union of all Grassmann varieties, i.e. the set of all subspaces of $\mathbb{F}_q^n$, is called the *projective space* and denoted by

$$\mathcal{P}_q(n) = \bigcup_{k=0}^{n} \mathcal{G}_q(k,n).$$

### A. The lattice point of view

The projective space $\mathcal{P}_q(n)$ forms a lattice with supremum "$+$" and infimum "$\cap$" which is called the *linear lattice* [4]. The dimension of subspaces defines a rank function satisfying the Jordan-Dedekind chain condition, i.e. $\mathcal{P}_q(n)$ is a JD-lattice. It is well-known that each JD-lattice $(L, \leq, \wedge, \vee, r, 0, 1)$ with partial order "$\leq$", infimum "$\wedge$", supremum "$\vee$", rank function $r$, zero-element $0 = \wedge_{x \in L} x$, and one-element $1 = \vee_{x \in L} x$ defines a metric lattice with a distance function $d$ (see [4]):

$$d(x,y) := r(x \vee y) - r(x \wedge y).$$

In the projective space setting, the corresponding metric is called the *subspace distance*: For two subspaces $\mathcal{U}, \mathcal{V} \in \mathcal{P}_q(n)$ we obtain:

$$d(\mathcal{U},\mathcal{V}) = \dim(\mathcal{U}+\mathcal{V}) - \dim(\mathcal{U} \cap \mathcal{V})$$
$$= \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2\dim(\mathcal{U} \cap \mathcal{V}).$$

In [18] Kötter and Kschischang suggested to use this metric subspace lattice for the purpose of coding in erroneous network communication. They defined a *subspace code* or *random network code* as a subset $\mathcal{C}$ of the projective space:

$$\mathcal{C} \subseteq \mathcal{P}_q(n).$$

A codeword of such a code corresponds to a subspace $\mathcal{U} \in \mathcal{C}$.

The minimum distance $d(\mathcal{C})$ of a subspace code $\mathcal{C}$ is defined in the usual way — as the smallest distance between any two elements of $\mathcal{C}$.

A special class of subspace codes are *constant dimension codes* [18]. These are simply subsets of the Grassmannian. If a constant dimension code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ has minimum distance $d(\mathcal{C})$, we call $\mathcal{C}$ an $[n, d(\mathcal{C}), |\mathcal{C}|, k]$-code.

A subspace code can be considered the $q$-analog of a binary block code [5], [6] as follows: The set $P(n)$ of all subsets of the $n$-set $N := \{0, \dots, n-1\}$ forms a JD-lattice with partial order "$\leq$", intersection of sets "$\cap$" as infimum operator, union

"$\cup$" as supremum, the order $|U|$ of a subset $U \in P(n)$ as rank function, the zero-element $\emptyset$, and the one-element $N$:

$$(P(n), \subseteq, \cap, \cup, |\cdot|, \emptyset, N).$$

Hence, the order of the symmetric difference of sets $U, V \in P(n)$,

$$d(U,V) = |U \cup V| - |U \cap V|,$$

defines a metric on $P(n)$. Since each subset $U \in P(n)$ can be represented by its characteristic vector $u = (u_0, \dots, u_{n-1}) \in \mathbb{F}_2^n$ ($u_i = 1$ if $i \in U$, otherwise $u_i = 0$), a binary block code corresponds to a subset

$$\mathcal{C} \subseteq P(n).$$

The given distance function $d$ is then nothing but the Hamming metric. A binary constant weight code is a subset $\mathcal{C} \subseteq P(n)$ whose elements $U \in \mathcal{C}$ have a fixed order $|U| = k$.

If we replace sets by subspaces and their orders by dimensions, we get the $q$-analog situation: Instead of the power set lattice $(P(n), \cap, \cup, |\cdot|, \emptyset, N)$ we use the projective space lattice

$$(\mathcal{P}_q(n), \leq, \cap, +, \dim, \{0\}, \mathbb{F}_q^n).$$

Then the $q$-analog of a binary block code is a subspace code and the $q$-analog of a binary constant weight code is a constant dimension code.

If $(L, \leq, \wedge, \vee, r, 0, 1)$ denotes a metric lattice, a bijective mapping $f : L \to L$ is called *isometric* on $L$ if and only if

$$d(f(x), f(y)) = d(x,y)$$

for all $x, y \in L$.

From lattice theory we know the following result, that order-preserving and order-reversing bijections on lattices define isometries [4], [6]:

**Lemma 1.** *Let $(L, \leq, \wedge, \vee, r, 0, 1)$ denote a metric lattice and let $f : L \to L$ denote a bijective mapping. Then the following equivalencies hold:*

1) *$f$ is order-preserving, i.e. $x \leq y \Leftrightarrow f(x) \leq f(y)$ for all $x, y \in L$, if and only if $r(f(x)) = r(x)$ for all $x \in L$ and $f$ is isometric on $L$.*
2) *$f$ is order-reversing, i.e. $x \leq y \Leftrightarrow f(y) \leq f(x)$ for all $x, y \in L$, if and only if $r(f(x)) = r(1) - r(x)$ for all $x \in L$ and $f$ is isometric on $L$.*

If $\mathrm{Aut}(L)$ denotes the set of all bijective order-preserving mappings on $L$ (also called *lattice automorphisms*) and $\mathrm{Anti}(L)$ denotes the set of all bijective order-reversing mappings on $L$ (also called *lattice anti-automorphisms*) the following lemma holds:

**Lemma 2.** *Let $(L, \leq, \wedge, \vee)$ be a lattice. Assume that there exists a mapping $f \in \mathrm{Anti}(L)$. Then*

$$\mathrm{Anti}(L) = \mathrm{Aut}(L) \circ f := \{g \circ f \mid g \in \mathrm{Aut}(L)\}.$$

*Proof:* We give a more general proof for partially ordered sets: Let $(A, \leq)$ respectively $(B, \preceq)$ two finite partially

ordered sets (posets). Then we define the set of poset isomorphisms, respectively the set of poset anti-automorphisms between $A$ and $B$:

$$\text{Iso}(A, B) := \{f : A \to B \mid f \text{ bijection},$$
$$f(x) \preceq f(y) \Leftrightarrow x \le y \ \forall x, y \in A\}$$

resp.

$$\text{AntiIso}(A, B) := \{f : A \to B \mid f \text{ bijection},$$
$$f(x) \preceq f(y) \Leftrightarrow y \le x \ \forall x, y \in A\}$$

Let $(A, \le)$ and $(B, \preceq)$ two posets. Assume that there exists a mapping $d \in \text{AntiIso}(A, B)$ Then we show that

$$\text{AntiIso}(A, A) = \text{Iso}(B, A) \circ d$$

⊆  Let $f \in \text{AntiIso}(L, L)$. Then $f^{-1} \in \text{AntiIso}(L, L)$ and we get the following equivalence, if we apply $d$:

$$x \le y \iff f^{-1}(y) \le f^{-1}(x)$$
$$\iff d(f^{-1}(x)) \preceq d(f^{-1}(y))$$
$$\iff (d \circ f^{-1})(x) \preceq (d \circ f^{-1})(y)$$

which means that $d \circ f^{-1} \in \text{Iso}(A, B)$. Hence there exists a mapping $g \in \text{Iso}(A, B)$ with $g = d \circ f^{-1}$. Applying $g^{-1} \in \text{Iso}(B, A)$ from the left and $f$ from the right to this identity yields $id = g^{-1} \circ d \circ f^{-1}$ respectively $f = g^{-1} \circ d \in \text{Iso}(B, A) \circ d$.

⊇  Let $f \in \text{Iso}(B, A)$. Then we have

$$x \le y \iff d(y) \preceq f(x)$$
$$\iff f(d(y)) \le f(d(x))$$
$$\iff (f \circ d)(y) \le (f \circ d)(x)$$

i.e. $f \circ d \in \text{AntiIso}(A, A)$. ∎

In case of the power set lattice, the set of all order-preserving bijective mappings on $P(n)$ are exactly the permutations on the $n$-set,

$$\text{Aut}(P(n)) = \text{Sym}(n) := \{\pi : N \to N \mid \pi \text{ bijection}\}.$$

In addition, an order-reversing mapping on $P(n)$ is defined by the setwise complement $\overline{U} = N \setminus U$, i.e. it satisfies

$$U \subseteq V \iff \overline{V} \subseteq \overline{U}.$$

In the setting of binary block codes, $Aut(P(n))$ is the set of the *permutation isometries*, or *linear isometries*, and the setwise complement corresponds to bit-flipping, i.e. a 1 becomes a 0 and vice versa. Denote by $\overline{\mathcal{C}}$ the code obtained by flipping the bits of a binary code $\mathcal{C}$. Then $\overline{\mathcal{C}}$ and $\mathcal{C}$ have the same minimum distance $d(\mathcal{C}) = d(\overline{\mathcal{C}})$, since the Hamming distance remains the same under bit-flipping, i.e. $d(\overline{u}, \overline{v}) = d(u, v)$.

In the case of the projective space lattice $\mathcal{P}_q(n)$ we know from the Fundamental Theorem of Projective Geometry (see [2], [3]) that the set of order-preserving bijections on $\mathcal{P}_q(n)$ corresponds exactly to the set of *semi-linear* mappings

$$\text{Aut}(\mathcal{P}_q(n)) = \Gamma\text{L}_n(\mathbb{F}_q) := \text{GL}_n(\mathbb{F}_q) \rtimes \text{Aut}(\mathbb{F}_q)$$

which is the semi-direct product of the *general linear* group $\text{GL}_n(\mathbb{F}_q)$ and the Galois group $\text{Aut}(\mathbb{F}_q)$.

If two codes are bijective with respect to a semi-linear mapping $f \in \Gamma\text{L}_n(\mathbb{F}_q)$ we call them *semi-linearly isometric*. If there exists $f \in \text{GL}_n(\mathbb{F}_q) \le \Gamma\text{L}_n(\mathbb{F}_q)$, such that $f$ maps one code to the other, the codes are called *linearly isometric*.

Furthermore, the *orthogonal complement* defines an order-reversing bijection on $\mathcal{P}_q(n)$,

$$\mathcal{U} \le \mathcal{V} \iff \mathcal{V}^\perp \le \mathcal{U}^\perp$$

and hence the *dual code* $\mathcal{C}^\perp := \{\mathcal{U}^\perp \mid \mathcal{U} \in \mathcal{C}\}$ defines a code with the same minimum distance as $\mathcal{C} \subseteq \mathcal{P}_q(n)$.

In particular, if $\mathcal{C}$ is a constant dimension $[n, d(\mathcal{C}), |\mathcal{C}|, k]$-code, the dual code $\mathcal{C}^\perp$ is an $[n, d(\mathcal{C}), |\mathcal{C}|, n-k]$-code. In fact, the dual of a constant dimension code is the $q$-analog of a flipped binary constant weight code.

### B. The incidence geometry point of view

Random network codes can be regarded as incidence structures in the projective space, therefore they are related to designs over finite fields [28]. A $t - (n, k, \lambda; q)$-design is a set $\mathcal{C}$ of $k$-subspaces, $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$, such that each $t$-subspace is contained in exactly $\lambda$ elements of $\mathcal{C}$. For the number of elements in such a design we get:

$$|\mathcal{C}| = \lambda \frac{\left[{n \atop t}\right]_q}{\left[{k \atop t}\right]_q}.$$

Each $t - (n, k, 1; q)$-design defines an optimal constant dimension code (cf. [17]) with parameters

$$\left[n, 2(k - t + 1), \frac{\left[{n \atop t}\right]_q}{\left[{k \atop t}\right]_q}, k\right].$$

So far the only non-trivial $t - (n, k, 1; q)$-designs are known for $t = 1$. Such a 1-design is called a *spread*, which exists if and only if $k$ divides $n$ (cf. [14], [21]). The corresponding optimal constant dimension code with parameters $[n, 2k, \frac{q^n-1}{q^k-1}, k]$ is called a *spread code* [22].

## III. THE GROUP ACTION POINT OF VIEW: ORBIT CODES

In this section we consider a third point of view: we derive random network codes from group actions—such codes are called *orbit codes* [23], [29]. We show, that this group theoretic approach yields a certain generalization of an ordinary linear code to random network codes. Both classes of codes, ordinary linear codes $C \le \mathbb{F}_q^n$ and orbit codes $\mathcal{C} \subseteq \mathcal{P}_q(n)$ can be defined by an orbit of a group action. If the group acting on the subspaces is cyclic we speak of *cyclic orbit codes* [30].

First we introduce the basic definitions and notation of groups acting on sets we need for our further investigations. The definitions and most results can be found in [7], [15].

### A. Basic definitions and properties of group actions

Let $G$ be a finite multiplicative group with one-element $1_G$ and let $X$ denote a finite set. A *group action* of $G$ on $X$ is a mapping

$$X \times G \longrightarrow X$$
$$(x, g) \longmapsto xg$$

such that $x1_G = x$ and $x(gg') = (xg)g'$ holds for all $x \in X$ and $g, g' \in G$. The fundamental property is that

$$x \sim_G x' : \Longleftrightarrow \exists g \in G : x' = xg$$

defines an equivalence relation on $X$. The induced equivalence classes are the *orbits* of $G$ on $X$. The orbit of $x \in X$ is abbreviated by

$$xG := \{xg \mid g \in G\}$$

and we denote the set of all orbits of $G$ on $X$ by

$$X/G := \{xG \mid x \in X\}.$$

A transversal of the orbits $X/G$, denoted by $\mathcal{T}(X/G)$, is a minimal subset of $X$ such that $X/G := \{xG \mid x \in \mathcal{T}(X/G)\}$, i. e. it is a set of representatives of the orbits.

Another useful tool in order to determine the corresponding orbit of an element $x \in X$ is the *canonizing mapping*:

$$\gamma_{\mathcal{T}(X/G)} : X \longrightarrow G$$
$$x \longmapsto g \text{ with } xg \in \mathcal{T}(X/G).$$

Two elements $x, x' \in X$ are in the same orbit, i.e. $xG = x'G$, if and only if

$$x\gamma_{\mathcal{T}(X/G)}(x) = x'\gamma_{\mathcal{T}(X/G)}(x').$$

The *stabilizer* of an element $x \in X$ is the set of group elements that fix $x$:

$$\mathrm{Stab}_G(x) := \{g \in G \mid xg = x\}.$$

Stabilizers are subgroups of $G$ having the property that the stabilizers of different elements of the same orbit are conjugated subgroups:

$$\mathrm{Stab}_G(xg) = g^{-1}\,\mathrm{Stab}_G(x)g.$$

The *Fundamental Lemma of group actions* [7], [15] says, that an orbit can be bijectively mapped onto the right cosets of the stabilizer:

$$\mathrm{Stab}_G(x)\backslash G \rightarrowtail xG$$
$$\mathrm{Stab}_G(x)g \mapsto xg.$$

In particular, if $\mathcal{T}(\mathrm{Stab}_G(x)\backslash G)$ denotes a transversal between $\mathrm{Stab}_G(x)$ and $G$, the mapping $\mathcal{T}(\mathrm{Stab}_G(x)\backslash G) \to xG, g \mapsto xg$ is also one-to-one. As an immediate consequence we obtain for the orbit size the equation:

**Proposition 3.**

$$|xG| = \frac{|G|}{|\mathrm{Stab}_G(x)|}$$

### B. Group actions and codes over metric sets

Now we switch to coding theory and assume $X$ to be a set admitting a metric function $d : X \times X \to \mathbb{R}$. A *code* is a subset $\mathcal{C} \subseteq X$. Its minimum distance is defined as

$$d(\mathcal{C}) := \min\{d(x, x') \mid x, x' \in \mathcal{C}, x \neq x'\}.$$

A *minimum distance decoder* of $\mathcal{C} \subseteq X$ is a maximum likelihood decoder

$$\mathrm{dec}_{\mathcal{C}} : X \longrightarrow \mathcal{C},$$

which maps an element $r \in X$ onto an element $c \in \mathcal{C}$ such that $d(c, r) \leq d(c', r)$ for all $c' \in \mathcal{C}$.

The following property is well-known:

**Lemma 4.** *Let* $\mathcal{C} \subseteq X$, $c \in \mathcal{C}$, *and let* $r \in X$. *If* $d(c, r) \leq \lfloor \frac{d(\mathcal{C})-1}{2} \rfloor$, *the minimum distance decoder* $\mathrm{dec}_{\mathcal{C}}$ *applied to* $r$ *finds the uniquely determined element* $c$.

From now on assume that the group elements act as an isometry on $X$, i. e.

$$d(xg, x'g) = d(x, x')$$

for all $x, x' \in X$ and $g \in G$. For two subsets $A, B \subseteq X$ we define the *intersubset distance* as

$$\hat{d}(A, B) = \min\{d(x, y) \mid x \in A, y \in B\}$$

which in fact defines a metric on the set of subsets of $X$. Using this intersubset distance we can define a metric on the set of orbits of $G$ on $X$:

$$\hat{d}(xG, yG) = \min\{d(xg, yh) \mid g, h \in G\}$$
$$= \min\{d(x, yhg^{-1}) \mid g, h \in G\}$$
$$= \min\{d(x, yg') \mid g' \in G\}.$$

**Lemma 5.** *The mapping* $\hat{d}$ *defines a metric function on the set of orbits* $X/G$.

*Proof:* The properties symmetry and positive definiteness of $\hat{d}$ follow directly from the properties of the metric $d$. The triangle inequality also holds: Let $x, y, z \in X$ and let $g, h \in G$ such that $\hat{d}(xG, yG) = d(x, yg)$ and $\hat{d}(yG, zG) = d(y, zh) = d(yg, zhg)$. Then we get

$$\hat{d}(xG, yG) + \hat{d}(yG, zG) = d(x, yg) + d(yg, zhg)$$
$$\geq d(x, z(hg))$$
$$\geq \hat{d}(xG, zG)$$

which completes the proof. ∎

**Definition 6.** Codes that are orbits of a group $G$ on a metric set $X$, are called *orbit codes*. If the group $G$ is cyclic we call them *cyclic orbit codes*.

We can evaluate the minimum distance of orbit codes more conveniently than considering all pairs of elements.

**Theorem 7.** *Let* $\mathcal{C} = xG$ *for an element* $x \in X$. *Then*

$$d(\mathcal{C}) = \min\{d(x, xg) \mid g \in \mathcal{T}(\mathrm{Stab}_G(x)\backslash G), g \notin \mathrm{Stab}_G(x)\}.$$

*Proof:* To evaluate the minimum distance we have to consider all $d(y, z)$ for all $y, z \in \mathcal{C}$ with $y \neq z$, i.e. $d(xg, xh) = d(x, xhg^{-1})$ for all $g, h \in G$ such that $xg \neq xh$, or equivalently $d(x, xg)$ for all $g \in G$ with $xg \neq x$. The Fundamental Lemma yields that it is sufficient to consider all $g$ from a transversal between the stabilizer $\mathrm{Stab}_G(x)$ and $G$ in order to run through the orbit $xG$. ∎

The following lemma describes a minimum distance decoder for orbit codes in terms of group actions using the canonizing mapping. The crucial fact is, that we have a transversal $\mathcal{T}(X/G) = \{x_0, x_1, \ldots, x_{\ell-1}\}$ of the orbits of $G$ on the set $X$, such that the distance of two transversal

elements $x_0$ and $x_i$ is the minimal distance between elements of the orbit code $\mathcal{C} = x_0 G$ and the orbit $x_i G$, i.e. the distance between $x_0$ and $x_i$ is the intersubset distance between the two sets $x_0 G$ and $x_i G$.

**Theorem 8.** *Let* $\mathcal{T}(X/G) = \{x_0, x_1, \ldots, x_{\ell-1}\}$ *be a transversal of the orbits, such that* $\hat{d}(x_0 G, x_i G) = d(x_0, x_i)$ *for all* $1 \leq i < \ell$ *and let* $\mathcal{C} = x_0 G$ *be the corresponding orbit code. Then the mapping*

$$\mathrm{dec}_{\mathcal{C}} : X \longrightarrow \mathcal{C}$$
$$r \longmapsto x_0 \gamma_{\mathcal{T}(X/G)}(r)^{-1}$$

*yields a minimum distance decoder, i.e.* $x_0 \gamma_{\mathcal{T}(X/G)}(r)^{-1} \in \mathcal{C}$ *is the closest codeword to* $r \in X$.

*Proof:* Assume that $r$ is in the orbit of $x_i$. The aim is now to find a codeword $c \in \mathcal{C} = x_0 G$, such that $d(c, r)$ is minimal. Let $g := \gamma_{\mathcal{T}(X/G)}(r)$ be the group element that maps $r$ onto the orbit representative $x_i$, i.e. $x_i = rg$. Then we obtain

$$d(x_0, x_i) = d(x_0, rg) = d(x_0 g^{-1}, r)$$
$$= d(x_0 \gamma_{\mathcal{T}(X/G)}(r)^{-1}, r).$$

Since we know that $d(x_0, x_i)$ is minimal between elements of $\mathcal{C} = x_0 G$ and $x_i G$ we get that $d(x_0 \gamma_{\mathcal{T}(X/G)}(r)^{-1}, r)$ is also minimal. Hence $c := x_0 \gamma_{\mathcal{T}(X/G)}(r)^{-1}$ is the closest codeword to $r$.

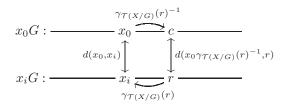This fact can easily be verified using Figure 1. ∎



Fig. 1. Visualization of the minimum distance decoder

### C. Isometric orbit codes

Let $H$ be a distance-preserving group acting *transitively* on the set $X$, i.e. $xH = X$ for all $x \in X$.

In this section we want to classify orbit codes that arise by subgroups $G$ of $H$, denoted by $G \leq H$. For this purpose we introduce the notion of isometry of orbit codes:

**Definition 9.** Two orbit codes $\mathcal{C}$ and $\mathcal{C}'$ defined by subgroups $G, G' \leq H$, i.e. $\mathcal{C} = xG$ and $\mathcal{C}' = x'G'$ for elements $x, x' \in X$, are called *$H$-isometric*, if there is a group element $h \in H$ mapping $\mathcal{C}$ onto $\mathcal{C}'$:

$$\mathcal{C}' = \mathcal{C}h := \{xh \mid x \in \mathcal{C}\}$$

**Theorem 10.** *The following properties hold:*
1) *Let* $G \leq H$ *and* $G' = h^{-1}Gh$ *for some* $h \in H$, *and* $x \in X$. *Then for* $x' = xh$ *the orbit codes* $\mathcal{C} = xG$ *and* $\mathcal{C}' = x'G'$ *are $H$-isometric.*
2) *Let* $\mathcal{C} = xG$ *and* $\mathcal{C}' = \mathcal{C}h$ *for some* $h \in H$, *i.e.* $\mathcal{C}$ *and* $\mathcal{C}'$ *are $H$-isometric. Then* $\mathcal{C}'$ *is an orbit code* $\mathcal{C}' = x'G'$ *with* $x' = xh$ *and* $G' = h^{-1}Gh$.

*Proof:* Both statements follow from

$$\mathcal{C}' = \{x'g' \mid g' \in G'\}$$
$$= \{xh(h^{-1}gh) \mid g \in G\}$$
$$= \{(xg)h \mid g \in G\}$$
$$= \mathcal{C}h.$$

∎

**Corollary 11.** *Two orbit codes are $H$-isometric, if and only if they arise from conjugate subgroups of $H$.*

Hence, it is sufficient to consider just one representative of each conjugacy class of *subgroups* of $H$, in order to classify by $H$-isometry. In the case of cyclic orbit codes we can even restrict to conjugacy classes of *group elements* of $H$.

**Lemma 12.** *Two cyclic subgroups $G, G'$ of $H$ are conjugate if and only if there exist some generators $g, g' \in H$ of these groups, i.e. $G = \langle g \rangle$ and $G' = \langle g' \rangle$, which are conjugate, i.e. $g' = h^{-1}gh$ for some $h \in H$.*

*Proof:*

$\boxed{\Leftarrow}$ Let $g' = h^{-1}gh$. Then

$$\langle g' \rangle = \langle (h^{-1}gh) \rangle$$
$$= \{(h^{-1}gh)^i \mid 0 \leq i < \ell\}$$
$$= \{h^{-1}g^i h \mid 0 \leq i < \ell\}$$
$$= h^{-1}\langle g \rangle h$$

i.e. $G' = h^{-1}Gh$.

$\boxed{\Rightarrow}$ Let $G' = h^{-1}Gh$ and $g$ a generator of $G$. Then

$$G' = h^{-1}Gh$$
$$= \{h^{-1}g^i h \mid 0 \leq i < \ell\}$$
$$= \{(h^{-1}gh)^i \mid 0 \leq i < \ell\}$$
$$= \langle h^{-1}gh \rangle$$

i.e. $h^{-1}gh$ is a generator of $G'$.

∎

**Corollary 13.** *Two cyclic orbit codes are $H$-isometric if and only if they arise by two cyclic subgroups $G_1, G_2 \leq H$ that are generated by conjugate elements of $H$. I. e. there exist $g_1, g_2 \in H$ such that*

$$G_1 = \langle g_1 \rangle, \quad G_2 = \langle g_2 \rangle$$

*and $g_2 = h^{-1}g_1 h$ for some $h \in H$.*

In order to furthermore study their properties, we introduce the notion of distance distribution of orbit codes which is adapted from the definition of weight enumerators of classical block codes.

**Definition 14.** Let $\mathcal{C} = xG$ be an orbit code. The *distance distribution* of $\mathcal{C}$ is the sequence $D_0, D_1, D_2, \ldots$ of natural numbers with

$$D_i := |\{y \in \mathcal{C} \mid d(x, y) = i\}|.$$

**Theorem 15.** *$H$-isometric orbit codes have the same distance distribution.*

*Proof:* Let $\mathcal{C} = xG$ and $\mathcal{C}' = \mathcal{C}h$ (for some $h \in H$) be two $H$-isometric orbit codes. Hence $h$ is a bijection between the two codes. Moreover,

$$d(xh, yh) = d(x, y)$$

for and $x, y \in \mathcal{C}$, i.e. the number of elements in $\mathcal{C}$ with a fixed distance from $x$ is the same as the number of elements in $\mathcal{C}'$ with that distance from $xh$. ∎

### D. Characterization of linear codes as orbit codes

Let $X = \mathbb{F}_q^n$ and let $C \leq \mathbb{F}_q^n$ be a linear code of dimension $k$. For any vector $v \in \mathbb{F}_q^n$ the mapping

$$\tau_v : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$$
$$x \longmapsto x\tau_v := x + v$$

defines a bijection. Since $C$ is an additive group the set

$$G = \{\tau_c \mid c \in C\}$$

also forms a group with respect to the composition. The map

$$\mathbb{F}_q^n \times G \longrightarrow \mathbb{F}_q^n$$
$$(x, \tau_c) \longmapsto x\tau_c = x + c$$

defines a group action, preserving the Hamming distance:

$$d(x, y) = d(x + c, y + c) = d(x\tau_c, y\tau_c).$$

Since the stabilizers $G_x$ of all elements $x \in \mathbb{F}_q^n$ are trivial, and the group has size $|G| = q^k$ the number of orbits is

$$\ell = |\mathbb{F}_q^n / G| = q^{n-k}.$$

Let $\mathcal{T}(\mathbb{F}_q^n / G) = \{x_0, x_1, \ldots, x_{\ell-1}\}$ be a transversal with $x_0 = 0$ satisfying the desired property

$$\hat{d}(x_0 G, x_i G) = \hat{d}(0G, x_i G) = d(0, x_i) = \text{weight}(x_i)$$

for all $1 \leq i < \ell$, i.e. the orbit representative $x_i$ has minimal weight within its orbit. Such an element is called *coset leader*.

If we take $x_0 = 0$ the corresponding orbit code $\mathcal{C} = x_0 G = 0G$ satisfies

$$\mathcal{C} = 0G = \{0\tau_c \mid c \in C\} = \{c \mid c \in C\} = C,$$

i.e. it is the linear code itself. Since the stabilizers $\text{Stab}_G(x)$ for all $x \in \mathbb{F}_q^n$ are trivial, a transversal between $G$ and $\text{Stab}_G(0)$ is the complete set $G$, i.e. $\mathcal{T}(\text{Stab}_G(0)\backslash G) = G$. Then Lemma 7 yields the formula:

$$d(\mathcal{C}) = \min\{d(0, 0\tau_c) \mid \tau_c \in \mathcal{T}(\text{Stab}_G(0)\backslash G), \tau_c \neq id\}$$
$$= \min\{d(0, c) \mid c \in C, c \neq 0\}.$$

If $r \in x_i G$ the element $\tau_{x_i - r} \in G$ is the canonical element of $x_i G$, i.e.

$$\gamma_{\mathcal{T}(\mathbb{F}_q^n / G)}(r) = \tau_{x_i - r},$$

since

$$y\tau_{x_i - r} = r + (x_i - r) = x_i.$$

It is obvious that $\tau_{x_i - r}^{-1} = \tau_{r - x_i}$. Hence, according to Lemma 8 the mapping

$$y \mapsto x_0 \gamma_{\mathcal{T}(\mathbb{F}_q^n / G)}(r)^{-1} = x_0 \tau_{x_i - r}^{-1}$$
$$= 0\tau_{r - x_i}$$
$$= 0 + (r - x_i)$$
$$= r - x_i$$

defines the minimum distance decoder. In fact, this corresponds exactly to the decoding procedure, which is known as *coset leader decoding*. The challenge here is to find the corresponding orbit $x_i G$ and hence the corresponding orbit representative $x_i$, which has minimal weight in its orbit. The determination of the orbit can be done by the evaluation of the syndrome, which is invariant on each orbit: If $\Delta$ denotes a check matrix of the linear code $C$ the equivalence holds:

$$x\Delta^t = y\Delta^t \iff xG = yG.$$

We now examine the $H$-isometry of these codes, where

$$H = \{\tau_c \mid c \in \mathbb{F}_q^n\}$$

acts on $\mathbb{F}_q^n$ the same way that $G$ does. According to Theorem 10 a code $\mathcal{C}' = x'G'$ with

$$x' = 0\tau_h = h, \quad G' = \tau_h^{-1} G \tau_h$$

is $H$-isometric to the orbit code $\mathcal{C} = 0G$. Since the group $H$ is commutative we get $G' = G$ and hence

$$\mathcal{C}' = hG = \{h + c \in C\} = h + C$$

if $G = \{\tau_c \mid c \in C\}$ is defined by a linear code $C \leq \mathbb{F}_q^n$. Finally, the codes which are $H$-isomorphic to a linear code $C \leq \mathbb{F}_q^n$ are the affine spaces $h + C$ for any $h \in \mathbb{F}_q^n$.

### E. Random network orbit codes

Now we consider random network codes arising from group actions which are simply called *orbit codes* and which were introduced in [29].

The general linear group of degree $n$, denoted by $\text{GL}_n$, is the set of all invertible $n \times n$-matrices with entries in $\mathbb{F}_q$. If we have to specify the underlying field we will write $\text{GL}_n(\mathbb{F}_q)$:

$$\text{GL}_n(\mathbb{F}_q) := \{A \in \mathbb{F}_q^{n \times n} \mid \text{rank}(A) = n\}.$$

In order to represent a $k$-subspace $\mathcal{U} \in \mathcal{G}_q(k, n)$ we use a *generator matrix* which is a $k \times n$-matrix $U$ whose rows form a basis of $\mathcal{U}$, i.e.

$$\mathcal{U} = \text{rs}(U) := \text{row space}(U) = \{xU \mid x \in \mathbb{F}_q^k\}.$$

Multiplication with $\text{GL}_n$-elements actually defines a group action from the right on the projective space $\mathcal{P}_q(n)$ by

$$\mathcal{P}_q(n) \times \text{GL}_n \longrightarrow \mathcal{P}_q(n)$$
$$(\mathcal{U}, A) \longmapsto \mathcal{U}A := \{vA \mid v \in \mathcal{U}\}.$$

Since any invertible matrix maps subspaces to subspaces of the same dimension and since two $k$-subspaces can be mapped onto each other by an invertible matrix, the orbit of the general linear group $\text{GL}_n$ on any $k$-subspace $\mathcal{U}$ is the whole set of

all $k$-subspaces. Thus, $\mathrm{GL}_n$ acts transitively on $\mathcal{G}_q(k, n)$. In particular, if $\mathcal{U}_k$ denotes the standard $k$-subspace generated by the first $k$ unit vectors, we get

$$\mathcal{U}_k\, \mathrm{GL}_n = \mathcal{G}_q(k, n).$$

Hence, the set of all orbits is

$$\mathcal{P}_q(n)/\,\mathrm{GL}_n = \{\mathcal{G}_q(0, n), \mathcal{G}_q(1, n), \ldots, \mathcal{G}_q(n, n)\}.$$

It is easy to verify that the stabilizer $\mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{U}_k)$ of the standard $k$-subspace $\mathcal{U}_k$ consists of all matrices of the form

$$\left( \begin{array}{c|c} X & 0 \\ \hline Y & Z \end{array} \right)$$

where $X \in \mathrm{GL}_k$, $Y \in \mathbb{F}_q^{n-k \times k}$ and $Z \in \mathrm{GL}_{n-k}$. Since every $k$-subspace $\mathcal{U}$ lies in the orbit of $\mathcal{U}_k$, say $\mathcal{U} = \mathcal{U}_k A$ for some $A \in \mathrm{GL}_n$, we get

$$\mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{U}) = A^{-1}\, \mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{U}_k) A.$$

If we take a subgroup $G$ of the general linear group $\mathrm{GL}_n$ and consider the orbits of $G$ on the set of all subspaces $\mathcal{P}_q(n)$ we obtain that the $GL_n$-orbits split into the $G$-orbits, such that $G$ induces an action on the Grassmannian $\mathcal{G}_q(k, n)$:

$$\mathcal{G}_q(k, n) \times G \longrightarrow \mathcal{G}_q(k, n)$$
$$(\mathcal{U}, A) \longmapsto \mathcal{U}A.$$

The corresponding stabilizers of this action are

$$\mathrm{Stab}_G(\mathcal{U}) = G \cap \mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{U}).$$

Now the definition of an orbit code in the setting of the projective space is straight-forward.

**Definition 16.** The orbits of a subgroup of the general linear group $\mathrm{GL}_n$ on the Grassmannian $\mathcal{G}_q(k, n)$ are called *(subspace) orbit codes*.

From Proposition 3 and Theorem 7 we can deduce:

**Theorem 17.** *Let $\mathcal{U} \in \mathcal{G}_q(k, n)$, $G \leq \mathrm{GL}_n$ and $\mathcal{C} = \mathcal{U}G$ be an orbit code.*

1) *The code $\mathcal{C}$ has size*

$$|\mathcal{C}| = \frac{|G|}{|\mathrm{Stab}_G(\mathcal{U})|} = \frac{|G|}{|G \cap \mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{U})|}.$$

2) *The minimum distance $d(\mathcal{C})$ of the code satisfies*

$$d(\mathcal{C}) = \min\{d(\mathcal{U}, \mathcal{U}A) \mid$$
$$A \in \mathcal{T}(\mathrm{Stab}_G(\mathcal{U})\backslash G), A \notin \mathrm{Stab}_G(\mathcal{U})\}.$$

3) *The stabilizers in $GL_n$ of different codewords $\mathcal{V}, \mathcal{W} \in \mathcal{C}$ are conjugated subgroups, i.e. there exists $A \in G$ with*

$$\mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{V}) = A^{-1}\, \mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{W})A.$$

*and*
$$\mathrm{Stab}_G(\mathcal{V}) = A^{-1}\, \mathrm{Stab}_G(\mathcal{W})A.$$

4) *In particular, $|\mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{V})| = |\mathrm{Stab}_{\mathrm{GL}_n}(\mathcal{W})|$, respectively $|\mathrm{Stab}_G(\mathcal{V})| = |\mathrm{Stab}_G(\mathcal{W})|$.*

As mentioned in Section II, the dual code $\mathcal{C}^{\perp} = \{\mathcal{U}^{\perp} \mid \mathcal{U} \in \mathcal{C}\}$ also defines a code with the same minimum distance as

the original code. Moreover, the dual of an orbit code forms an orbit code as well [29]:

**Theorem 18.** *Let $\mathcal{U} \in \mathcal{G}_q(k, n)$, $G$ a subgroup of $\mathrm{GL}_n$ and $\mathcal{C} = \mathcal{U}G$ be an orbit code. Then the dual satisfies $\mathcal{C}^{\perp} = (\mathcal{U}^{\perp})G^t$ where $G^t = \{A^t \mid A \in G\}$.*

*Proof:* The proof immediately follows from the identity $(\mathcal{U}A)^{\perp} = (\mathcal{U}^{\perp})(A^{-1})^t$. ∎

Denote by $D_0(\mathcal{C}), D_2(\mathcal{C}), \ldots, D_{2k}(\mathcal{C})$ the distance distribution of the orbit code $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ and define the distance enumerator polynomial of an orbit code $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ by

$$\mathcal{D}_{\mathcal{C}}(x, y) := \sum_{i=0}^{k} D_{2i}(\mathcal{C}) x^i y^{k-i}.$$

Then one can easily derive the analogue of the MacWilliams identity:

**Theorem 19.**
$$\mathcal{D}_{\mathcal{C}}(x, y) = \mathcal{D}_{\mathcal{C}^{\perp}}(x, y)$$

*Proof:* The statement follows from the fact that $d(\mathcal{U}^{\perp}, \mathcal{V}^{\perp}) = d(\mathcal{U}, \mathcal{V})$ for any $\mathcal{U}, \mathcal{V} \in \mathcal{G}_q(k, n)$, which implies that $D_{2i}(\mathcal{C}) = D_{2i}(\mathcal{C}^{\perp})$ for all $i = 0, \ldots, k$. ∎

## IV. CLASSIFICATION OF CYCLIC ORBIT CODES

As described in section III-C isometric network orbits codes arise from the different conjugacy classes of subgroups of the general linear group $H = \mathrm{GL}_n$. Moreover, the isometric cyclic orbit codes correspond to the different conjugacy classes of elements of $\mathrm{GL}_n$. A canonical transversal of all these conjugacy classes can be obtained from the different *rational canonical forms* of invertible matrices. In this section we want to specify these matrix representatives and give some properties of the groups and orbit codes generated by these matrices in canonical forms.

### A. Rational canonical forms and conjugacy classes

For simplicity, in this section we abbreviate the notation of polynomials to $p \in \mathbb{F}_q[x]$.

**Definition 20.** Let $p = p_0 + p_1 x + \ldots + p_{n-1} x^{n-1} + x^n \in F_q[x]$. The *companion matrix* of $p$ is

$$M_p := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & & 1 \\ -p_0 & -p_1 & -p_2 & \cdots & -p_{n-1} \end{pmatrix} \in \mathbb{F}_q^{n \times n}.$$

**Definition 21.** Let $p(x) \in \mathbb{F}_q[x]$ with $p(0) \neq 0$. Then the least integer $e \in \mathbb{N}$ such that $p(x)$ divides $x^e - 1$ is called the *order* of $p(x)$.

The interested reader can find more information related to the previous definitions in [20].

We characterize conjugacy classes of elements of $\mathrm{GL}_n$ by the rational canonical forms. The following result can be found in [13, Chapter 6.7].

**Theorem 22.** *Let $A \in \mathrm{GL}_n$. Then there exist a transformation matrix $L \in \mathrm{GL}_n$, distinct monic irreducible polynomials $p_1, \ldots, p_m \in \mathbb{F}_q[x]$ and integer partitions $e_1, \ldots, e_m$ of natural numbers $n_1, \ldots, n_m$, $n = \sum_i n_i$,*

$$e_i = (e_{i,1}, \ldots, e_{i,r_i}) \text{ with } e_{i,1} \geq \ldots \geq e_{i,r_i} \text{ and } n_i = \sum_j e_{i,j}$$

*such that*

$$L^{-1}AL =$$
$$\mathrm{diag}(M_{p_1^{e_{1,1}}}, \ldots, M_{p_1^{e_{1,r_1}}}, \ldots, M_{p_m^{e_{m,1}}}, \ldots, M_{p_m^{e_{m,r_m}}})$$

*forms a block diagonal matrix with companion matrices $M_{p_i^{e_{i,j}}}$ of the polynomials $p_i^{e_{i,j}}$. Moreover, this matrix is unique (up to ordering of the polynomials) for any choice of $A \in \mathrm{GL}_n$. Hence, we call this block diagonal matrix the* rational canonical form *of $A$ and we write*

$$\mathrm{RCF}(A) := L^{-1}AL.$$

*The polynomials $p_i^{e_{i,j}}$ are called* elementary divisors *of $A$.*

**Corollary 23.** *Two matrices $A, B \in \mathrm{GL}_n$ are conjugate if and only if $\mathrm{RCF}(A) = \mathrm{RCF}(B)$.*

The conjugacy classes of elements in $\mathrm{GL}_n$ are determined by the finite lists of $m$ distinct monic irreducible polynomials $p_1, \ldots, p_m$ and the $m$ partitions $e_1, \ldots, e_m$ of the numbers $n_1, \ldots, n_m$ such that $n = \sum_i n_i$.

If we consider conjugation of subgroups, which is what matters for the consideration of isometry of orbit codes, we show in the following that the number $m$ and the partitions $e_1, \ldots, e_m$ and the order of the polynomials $p_1, \ldots, p_m$ are invariant on the generators of subgroups of the same conjugacy class of subgroups. Hence, the choice of irreducible polynomials $p_1, \ldots, p_m$ is based only on their order.

More formally, assume that the list of partitions $e_1, \ldots, e_m$ is in a unique ordering (e.g. lexicographically increasing), and let $o_1, \ldots, o_m \in \mathbb{N}$ be the orders of the polynomials $p_1, \ldots, p_m$, then the couple given by the ordered vector of all partitions

$$e(A) := (e_1, \ldots, e_m)$$

and by the vector

$$o(A) := (o_1, \ldots, o_m)$$

will be called the *matrix type* of the rational canonical form of a matrix $A$.

**Corollary 24.** *Let $A, B \in \mathrm{GL}_n$ be conjugate matrices. Then the rational canonical forms of both matrices have the same type, i.e.*

$$e(A) = e(B) \text{ and } o(A) = o(B).$$

**Lemma 25.** *The matrix type is constant on the set of all generators of the same cyclic group:*

$$\langle A \rangle = \langle B \rangle \implies e(A) = e(B) \text{ and } o(A) = o(B).$$

*Proof:* First we show the case where $A$ has a unique elementary divisor. At the end of the proof we will give the main remark that implies the generalized statement.

From the unique divisor of $A$, it follows that the characteristic and the minimal polynomial of $A$ are both $p^e \in \mathbb{F}_q[x]$ where $p \in \mathbb{F}_q[x]$ is irreducible. Define $k := n/e$ and let $\mathbb{F}_{q^k} := \mathbb{F}_q[x]/(p)$ be the splitting field of the polynomial $p$ and $\mu \in \mathbb{F}_{q^k}$ a primitive element of it. There exists a $j \in \mathbb{N}$ such that $p = \prod_{u=0}^{k-1}(x - \mu^{jq^u})$. Since $p^e$ is the characteristic and the minimal polynomial of $A$, we obtain that the Jordan normal form of $A$ over $\mathbb{F}_{q^k}$ is

$$J_A = \mathrm{diag}\left(J_{A,\mu^j}^e, \ldots, J_{A,\mu^{jq^{k-1}}}^e\right)$$

where $J_{A,\mu^{jq^u}}^e \in \mathrm{GL}_e(\mathbb{F}_{q^k})$ is a unique Jordan block with diagonal entries $\mu^{jq^u}$ for $0 \leq u < k$.

By the Jordan normal form of $A$ it follows that for every $i \in \mathbb{N}$ the characteristic polynomial of $A^i$ is

$$p_{A^i} = \left(\prod_{u=0}^{k-1} x - \mu^{ijq^u}\right)^e.$$

Since $B$ is a generator of $\langle A \rangle$, there exists an $i$ with $\gcd(i, |\langle A \rangle|) = 1$ such that $B = A^i$. It follows that $p_{A^i} \in \mathbb{F}_q[x]$ is a monic irreducible polynomial whose order is the same as the one of $p$.

In order to conclude that $p_{A^i}^e$ is the unique elementary divisor of $A^i$, we consider its rational canonical form. Without loss of generality, assume the rational canonical form of $A^i$ to be

$$\mathrm{RCF}(A^i) = \mathrm{diag}\left(M_{p_{A^i}^{e_1}}, M_{p_{A^i}^{e_2}}\right)$$

where $e = e_1 + e_2$. For any $j \in \mathbb{N}$ we obtain that the matrix $\mathrm{RCF}((\mathrm{RCF}(A^i))^j)$ is a block diagonal matrix with at least two blocks. Let $j \in \mathbb{N}$ such that $ij \equiv 1 \pmod{|\langle A \rangle|}$ and $L \in \mathrm{GL}_n$ be a matrix such that $\mathrm{RCF}(A^i) = L^{-1}A^iL$, then

$$(\mathrm{RCF}(A^i))^j = (L^{-1}A^iL)^j = L^{-1}AL$$

implying that

$$\mathrm{RCF}(A) = \mathrm{RCF}((\mathrm{RCF}(A^i))^j).$$

This leads to a contradiction since $\mathrm{RCF}(A) = M_{p^e}$ has only one block. We conclude that $p_{A^i}^e$ is the elementary divisor of $A^i$.

If $m > 1$ the only difference is the choice of the splitting field. If $p_1, \ldots, p_m$ are the distinct monic irreducible polynomials related to $\mathrm{RCF}(A)$, then the splitting field on which the proof is based is $\mathbb{F}_q[x]/(\prod_{t=1}^m p_i)$. ∎

Due to this result, the following definition is well-defined. If $G = \langle A \rangle$ denotes a cyclic subgroup of $\mathrm{GL}_n$, the type of the cyclic group $G$ is defined by

$$e(G) := e(A) \text{ and } o(G) := o(A).$$

**Theorem 26.** *Let $G, G'$ be two cyclic subgroups of $\mathrm{GL}_n$. Then they are conjugate if and only if they have the same group type:*

$$G, G' \text{ conjugate} \iff e(G) = e(G') \text{ and } o(G) = o(G').$$

*Proof:*

$\boxed{\Rightarrow}$   Follows from Corollary 24 and Lemma 25.

$\boxed{\Leftarrow}$   Let $G = \langle A \rangle$ and $G' = \langle A' \rangle$, we obtain that

$$e(A) = e(A') \text{ and } o(A) = o(A').$$

Let $p_{A,1}, \ldots p_{A,m}, p_{A',1}, \ldots p_{A',m}, \in \mathbb{F}_q[x]$ be the bases of the elementary divisors of $A$ and $A'$, respectively. Since $o(A) = o(A')$, let $\mathbb{F}$ be the unique splitting field of $(\prod_{t=1}^r p_{A,t})(\prod_{t=1}^r p_{A',t})$, and $\mu \in \mathbb{F}$ a primitive element of it.

Let $d_j := \deg p_{A,j}$ for $j = 1, \ldots, m$. Then, there exist $i_1, \ldots, i_m \in \mathbb{N}$ such that

$$p_{A,j} = \prod_{u=0}^{d_j - 1}(x - \mu^{i_j q^u})$$

for $j = 1, \ldots, m$. The same holds for the matrix $A'$, i.e. there exist $i'_1, \ldots, i'_m \in \mathbb{N}$ such that

$$p_{A',j} = \prod_{u=0}^{d_j - 1}(x - \mu^{i'_j q^u})$$

for $j = 1, \ldots, m$. By the condition on the orders, there exists a unique $i \in \mathbb{N}$ such that

$$i_j \equiv i \cdot i'_j \pmod{o_j}$$

for $j = 1, \ldots, m$. We obtain that $p_{(A')^i,j} = p_{A,j}$ which combined with the condition $e(A) = e(A')$ implies that $\mathrm{RCF}((A')^i) = \mathrm{RCF}(A)$, i.e. $A$ and $(A')^i$ are conjugate.

∎

In order to obtain a transversal of the conjugacy classes of all cyclic subgroups of $\mathrm{GL}_n$ we have to consider their group types. These correspond to all different ordered lists of partitions $(e_1, \ldots, e_m)$, $e_i = (e_{i,1}, \ldots, e_{i,r_i})$, such that $\sum_{i,j} e_{i,j} = n$ together with possible orders $(o_1, \ldots, o_m)$.

Hence, we can uniquely represent the conjugacy class of a cyclic subgroup of $\mathrm{GL}_n$ by a rational canonical form where the irreducible polynomials of the elementary divisors have the given degrees and orders.

### B. Cyclic orbit codes from block matrices

In order to simplify the following statements, let $M := \mathrm{diag}(M_1, \ldots, M_t) \in \mathrm{GL}_n$ be a block diagonal matrix where the $M_i$ are the companion matrices of the polynomials $p_i^{e_i} \in \mathbb{F}_q[x]$, the $p_i$ are monic irreducible polynomials, and $n_i = \deg(p_i^{e_i})$.

**Lemma 27.** *Let* $U = \mathrm{rs}(U_1, \ldots, U_t) \in \mathcal{G}_q(k,n)$, $r_i := \min\{r \in \mathbb{N} \mid \mathrm{rs}(U_i)M_i^r = \mathrm{rs}(U_i)\}$ *and* $s_i := \min\{s \in \mathbb{N} \mid U_i M_i^s = U_i\}$ *for* $i = 1, \ldots, t$. *Then the smallest* $g \in \mathbb{N}$ *with*

$$\mathrm{Stab}_{\langle M \rangle}(\mathcal{U}) = \langle M^g \rangle$$

*fulfills*

$$\mathrm{lcm}(r_i \mid i \in \{1, \ldots, t\}) \mid g \mid \mathrm{lcm}(s_i \mid i \in \{1, \ldots, t\}).$$

*Proof:* Let

$$g := \min\{l \in \{0, \ldots, |\langle M \rangle| - 1\} \mid \mathrm{Stab}_{\langle M \rangle}(\mathcal{U}) = \langle M^l \rangle\}.$$

It holds that

1) $\mathrm{lcm}(r_i \mid i \in \{1, \ldots, t\}) \mid g$: Since $M^g \in \mathrm{Stab}_{\langle M \rangle}(\mathcal{U})$, then there exists an $N \in \mathrm{GL}_k$ such that

$$
\begin{aligned}
(U_1, \ldots, U_t) &= N(U_1, \ldots, U_t)M^g \\
&= (NU_1 M_1^g, \ldots, NU_t M_t^g).
\end{aligned}
$$

It follows that $U_i = NU_i M_i^g$ which means that $M_i^g \in \mathrm{Stab}_{\langle M_i \rangle}(\mathcal{U}_i)$, i.e., $r_i \mid g$ for any $i \in \{1, \ldots, t\}$.

2) $g \mid \mathrm{lcm}(s_i \mid i \in \{1, \ldots, t\})$ since, by definition of the $s_i$, $M^{\mathrm{lcm}(s_i \mid i \in \{1, \ldots, t\})} \in \mathrm{Stab}_{G_M}(\mathcal{U})$.

∎

**Proposition 28.** *Let* $k_i \leq n_i$, $U_i \in \mathbb{F}_q^{k_i \times d_i}$ *be matrices with full rank,* $\mathcal{U} := \mathrm{rs}(U) \in \mathcal{G}_q(k,n)$ *where* $U = \mathrm{diag}(U_1, \ldots, U_t)$, $\mathcal{C} = \mathcal{U}\langle M \rangle$ *and* $\mathcal{C}_i := \mathrm{rs}(U_i)\langle M_i \rangle$. *It holds that*

$$|\mathcal{C}| = \mathrm{lcm}(|\mathcal{C}_i| \mid i \in \{1, \ldots, t\})$$

*and*

$$d(\mathcal{C}) \geq \min_{i \in \{1, \ldots, t\}}\{d(\mathcal{C}_i)\}.$$

*Moreover, we can distinguish the following cases:*

- *If* $\gcd(|\mathcal{C}_i|, |\mathcal{C}_j|) = 1$ *for all* $i \neq j$, *then*

$$d(\mathcal{C}) = \min_{i \in \{1, \ldots, t\}}\{d(\mathcal{C}_i)\}.$$

- *If* $J = \{i \in \{1, \ldots, t\} \mid |\mathcal{C}_i| = |\mathcal{C}|\} \neq \emptyset$, *then*

$$d(\mathcal{C}) \geq \sum_{j \in \{1, \ldots, t\} \setminus J} d(\mathcal{C}_j).$$

*Proof:*

1) Let us first derive the cardinality of $\mathcal{C}$. Let $j := \min\{i \in \mathbb{N} \mid \mathcal{U} = \mathcal{U}M^i\}$. Then

$$
\begin{aligned}
\mathrm{rank}\begin{pmatrix} U \\ UM^j \end{pmatrix} &= \mathrm{rank}\begin{pmatrix} \mathrm{diag}(U_1, \ldots, U_t) \\ \mathrm{diag}(U_1 M_1^j, \ldots, U_t M_t^j) \end{pmatrix} \\
&= \sum_{i=1}^t \mathrm{rank}\begin{pmatrix} U_i \\ U_i M_i^j \end{pmatrix} = k.
\end{aligned}
$$

Since $\mathrm{rank}\begin{pmatrix} U_i \\ U_i M_i^j \end{pmatrix} \geq k_i$ for all $i \in \{1, \ldots, t\}$, it follows that $\mathrm{rs}(U_i) = \mathrm{rs}(U_i)M^j$, implying that $|\mathcal{C}_i|$ divides $j$ for all $i \in \{1, \ldots, t\}$. By minimality we obtain the formula of the cardinality.

2) To show the bound on the minimum distance assume without loss of generality that $d(\mathcal{C}_1) \leq d(\mathcal{C}_i)$ for $i \in \{1, \ldots, t\}$ and $d_1 \in \mathbb{N}$ such that

$$d_1 = \max_{1 \leq j < |\mathcal{C}_1|}\left\{\dim(\mathrm{rs}(U_1) \cap \mathrm{rs}(U_1)M_1^j)\right\}.$$

For $1 \leq j < |\mathcal{C}|$, it holds that

$$
\begin{aligned}
\mathrm{rank}\begin{pmatrix} U \\ UM^j \end{pmatrix} &= \sum_{i=1}^t \mathrm{rank}\begin{pmatrix} U_i \\ U_i M_i^j \end{pmatrix} \\
&\geq 2k_1 - d_1 + \sum_{i=2}^t k_i = k + k_1 - d_1.
\end{aligned}
$$

It follows that

$$d(\mathcal{C}) = 2 \min_{1 \le j < |\mathcal{C}|} \left\{ \operatorname{rank} \begin{pmatrix} U \\ UM^j \end{pmatrix} \right\} - 2k$$
$$\ge 2(k + k_1 - d_1) - 2k = 2k_1 - 2d_1 = d(\mathcal{C}_1).$$

3) The inequality becomes an equality if $\gcd(|\mathcal{C}_i|, |\mathcal{C}_j|) = 1$ for any $i \ne j$, since there exists a $1 \le g < |\mathcal{C}|$ such that

$$g \equiv g_1 \pmod{|\mathcal{C}_1|} \text{ and } g \equiv 0 \pmod{|\mathcal{C}_j|}$$

for $j > 1$. It follows that $d(\mathcal{U}, \mathcal{U}M^g) = d(\mathcal{C}_1)$.

4) If instead $J := \{i \in \{1, \ldots, t\} \mid |\mathcal{C}_i| = |\mathcal{C}|\}$ is non-empty, then, for any $1 \le j < |\mathcal{C}|$, it holds that

$$\operatorname{rank} \begin{pmatrix} U \\ UM^j \end{pmatrix} \ge \sum_{i \in J} k_i + \sum_{i \notin J} (2k_i - d_i) = k + \sum_{i \notin J} (k_i - d_i)$$

where $d_i = \max_{1 \le j < |\mathcal{C}_i|} \left\{ \dim(\operatorname{rs}(\bar{U}_i) \cap \operatorname{rs}(\bar{U}_i)M_i^j) \right\}$. This implies that

$$d(\mathcal{C}) \ge \sum_{j \notin J} d(\mathcal{C}_j).$$

∎

**Proposition 29.** *Let* $\mathcal{U} := \operatorname{rs}(U_1, \ldots, U_t) \in \mathcal{G}_q(k, n)$ *where* $k \le n_i$ *and* $U_i \in \mathbb{F}_q^{k \times n_i}$ *are matrices having full rank. Define*

$$\mathcal{C} := \mathcal{U}\langle M \rangle \subset \mathcal{G}_q(k, n) \text{ and } \mathcal{C}_i := \operatorname{rs}(U_i)\langle M_i \rangle \subset \mathcal{G}_q(k, n_i).$$

*It holds that*

$$d(\mathcal{C}) \ge \min_{i \in \{1, \ldots, t\}} \{d(\mathcal{C}_i)\}.$$

*Proof:* For any $g \in \{1, \ldots, |\mathcal{C}| - 1\}$ the following properties hold:

1) If $v = (v_1, \ldots, v_t) \in \mathcal{U} \cap \mathcal{U}M^g$ where $v_i \in \mathbb{F}_q^{n_i}$ then $v_i \in \operatorname{rs}(U_i) \cap \operatorname{rs}(U_i)M_i^g$ for $i \in \{1, \ldots, t\}$.
2) There exists $j \in \{1, \ldots, t\}$ such that $\operatorname{rs}(U_j) \ne \operatorname{rs}(U_j)M_j^g$.

It follows that

$$\max_g \{\dim(\mathcal{U} \cap \mathcal{U}M^g)\} \le$$

$$\max_i \left\{ \max_g \{\dim(\operatorname{rs}(U_i) \cap \operatorname{rs}(U_i)M_i^g) \mid \operatorname{rs}(U_i) \ne \operatorname{rs}(U_i)M_i^g\} \right\}$$

which implies that $d(\mathcal{C}) \ge \min_{i \in \{1, \ldots, t\}} \{d(\mathcal{C}_i)\}$. ∎

**Example 30.** Let $p_1 = x^4 + x + 1, p_2 = x^6 + x + 1 \in \mathbb{F}_2[x]$ and $M_1, M_2$ the respective companion matrices of $p_1, p_2$. Let

$$U_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \ U_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

and $\mathcal{C}_1 = \operatorname{rs}(U_1)\langle M_1 \rangle$ and $\mathcal{C}_1 = \operatorname{rs}(U_2)\langle M_2 \rangle$. It holds that $|\mathcal{C}_1| = 5, |\mathcal{C}_2| = 21$ and $d(\mathcal{C}_1) = d(\mathcal{C}_2) = 4$.

1) *Proposition 28:*
   Let $\mathcal{U} = \operatorname{rs}\begin{pmatrix} U_1 & 0 \\ 0 & U_2 \end{pmatrix} \in \mathcal{G}_2(4, 10)$ and $M = \operatorname{diag}(M_1, M_2)$, then $|\mathcal{C}| = 105$ and $d(\mathcal{C}) = 4$.
2) *Proposition 29:*
   Let $\mathcal{U} = \operatorname{rs}(U_1 \ U_2)$, $M = \operatorname{diag}(M_1, M_2)$ and $\mathcal{C} = \mathcal{U}\langle M \rangle$, then

$$|\mathcal{C}| = 315 \text{ and } d(\mathcal{C}) = 4.$$

## V. CARDINALITY AND MINIMUM DISTANCE OF CYCLIC ORBIT CODES

In the previous section we investigated the cyclic subgroups of $\mathrm{GL}_n$ to classify the respective orbit codes. To compute the minimum distance and cardinality of a given cyclic orbit code we also need to take the starting point of that orbit into account. In this section we will show how to compute these parameters using the polynomial extension field representation of the elements of that starting point.

We will explain in detail the case of irreducible cyclic orbit codes and give some remarks in the end how to generalize this to arbitrary cyclic subgroups of $\mathrm{GL}_n$.

### A. Irreducible cyclic orbit codes

**Definition 31.** 1) A matrix $A \in \mathrm{GL}_n$ is called *irreducible* if $\mathbb{F}_q^n$ contains no non-trivial $A$-invariant subspace, otherwise it is called *reducible*.
2) A non-trivial subgroup $G \le \mathrm{GL}_n$ is called *irreducible* if $\mathbb{F}_q^n$ contains no non-trivial $G$-invariant subspace, otherwise it is called *reducible*.

A cyclic group is irreducible if and only if its generator matrix is irreducible. Moreover, an invertible matrix is irreducible if and only if its characteristic polynomial is irreducible. The rational canonical form of such an invertible matrix is the companion matrix of its characteristic polynomial.

It follows that any cyclic irreducible subgroup of $\mathrm{GL}_n$ is conjugate to a group generated by a companion matrix of an irreducible polynomial. Moreover, we know from Theorem 26 that groups generated by companion matrices of an irreducible polynomial of the same order are conjugate and from Lemma 10 that orbit codes defined by conjugate groups are isometric.

Therefore it is sufficient to characterize the orbits of cyclic groups generated by companion matrices of irreducible polynomials of degree $n$ of different orders.

We first need the following definitions and results on irreducible polynomials over finite fields.

Let $p(x) = p_0 + p_1 x + \ldots + p_{n-1} x^{n-1} + x^n$ be a monic irreducible polynomial of degree $n$ over the finite field $\mathbb{F}_q$.

In the finite field $\mathbb{F}_q[x]/(p(x))$, the modular multiplication of an element $v(x) = v_0 + v_1 x + \ldots + v_{n-1} x^{n-1}$ by the fixed polynomial $x$ yields

$$w(x) = v(x) \cdot x \pmod{p(x)}$$
$$= -v_{n-1} p_0 + \sum_{i=1}^{n-1} (v_{i-1} - v_{n-1} p_i) x^i.$$

Using a vector representation of $\mathbb{F}_q[x]/(p(x))$, the modular multiplication by $x$, $w(x) = v(x) \cdot x \pmod{p(x)}$ yields a linear mapping

$$(w_0, w_1, \ldots, w_{n-1}) = (v_0, v_1, \ldots, v_{n-1}) M_p$$

where $M_p$ is the companion matrix of $p(x)$ as defined in Definition 20.

If $p(x)$ is a *primitive* polynomial, i.e. the minimal polynomial of a multiplicative generator $\alpha$ of $\mathbb{F}_{q^n}^* := \mathbb{F}_{q^n} \setminus \{0\}$, the group generated by $M_p$ has order $q^n - 1$ and is known as the *Singer group*. This notation is used e.g. by Kohnert et al.

in their network code construction [8], [17]. Elsewhere $M_p$ is called *Singer cycle* or *cyclic projectivity* (e. g. in [14]).

If we substitute the indeterminate $x$ in the polynomials $v \in \mathbb{F}_q$ by the generator $\alpha \in \mathbb{F}_{q^n}^*$, the modular multiplication with $x$ corresponds to the multiplication with $\alpha$ and hence to multiplication with the companion matrix $M_p$:

**Lemma 32.** *Let $p(x)$ be an irreducible polynomial over $\mathbb{F}_q$ of degree $n$ and $P$ its companion matrix. Furthermore let $\alpha \in \mathbb{F}_{q^n}^*$ be a root of $p(x)$ and $\phi$ be the canonical homomorphism*

$$\phi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_{q^n}$$

$$(v_0, \ldots, v_{n-1}) \longmapsto \sum_{i=0}^{n-1} v_i \alpha^i.$$

*Then the multiplication with $M_p$ resp. $\alpha$ commutes with the mapping $\phi$, i. e. for all $v \in \mathbb{F}_q^n$ we get*

$$\phi(v M_p) = \phi(v)\alpha.$$

**Definition 33.** A *multiset* is a generalization of the notion of set in which members are allowed to appear more than once. To distinguish it from usual sets $\{x \in X\}$ we will denote multisets by $\{\{x \in X\}\}$. The number of times an element $x$ belongs to the multiset $X$ is the *multiplicity* of that element, denoted by $m_X(x)$.

We will first investigate the simpler case of primitive companion matrices and then generalize it to arbitrary irreducible cyclic orbit codes.

*Primitive Generator:* For this part of the paper let $p(x) \in \mathbb{F}_q[x]$ always be a primitive polynomial of degree $n$ (i. e. the order of $p(x)$ is $q^n - 1$) and $\alpha$ be a root of it. Thus $\alpha$ is a primitive element of $\mathbb{F}_{q^n}$. It follows that for any non-zero element $u \in \mathbb{F}_q^n$ there exists an $i \in \mathbb{Z}_{q^n-1}$ such that $\phi(u) = \alpha^i$.

The following fact is a generalization of Lemma 1 from [17] and has been formulated in a similar manner in [30].

**Theorem 34.** *Assume $\mathcal{U} = \{0, u_1, \ldots, u_{q^k-1}\} \in \mathcal{G}_q(k, n)$, where $u_i \in \mathbb{F}_q^n \setminus \{0\}$ and let $b_i \in \mathbb{Z}_{q^n-1}$ such that*

$$\phi(u_i) = \alpha^{b_i} \qquad \forall i = 1, \ldots, q^k - 1.$$

*Let $d$ be minimal such that any element of the set*

$$D := \{\{b_m - b_l \mod q^n - 1 \mid l, m \in \mathbb{Z}_{q^k-1}, l \neq m\}\}$$

*has multiplicity less than or equal to $q^d - 1$, i. e. a quotient of two elements in the field representation appears at most $q^d - 1$ times in the set of all pairwise quotients. If $d < k$ then the orbit of the group generated by the companion matrix $P$ of $p(x)$ on $\mathcal{U}$ is an orbit code of cardinality $q^n - 1$ and minimum distance $2k - 2d$.*

*Proof:* In field representation the elements of the orbit code are:

$$C_0 = \{\alpha^{b_1}, \alpha^{b_2}, \ldots, \alpha^{b_{q^k-1}}\} \cup \{0\}$$
$$C_1 = \{\alpha^{b_1+1}, \alpha^{b_2+1}, \ldots, \alpha^{b_{q^k-1}+1}\} \cup \{0\}$$
$$\vdots$$
$$C_{q^n-2} = \{\alpha^{b_1+q^n-2}, \ldots, \alpha^{b_{q^k-1}+q^n-2}\} \cup \{0\}$$

First we compute the minimum distance of the code. We know from Theorem 17 that it suffices to compute the minimum distance and therefor the intersection of $C_0$ with $C_h$ for $h = 1, \ldots, q^n - 2$. A non-zero element $\alpha^{b_i} \in C_0$ is also in $C_h$ if and only if

$$\alpha^{b_i} = \alpha^{b_j + h} \quad \text{for some } j \in \{1, \ldots, q^k - 1\}$$

$$\iff b_i - b_j \equiv h \mod q^n - 1.$$

But by assumption there are at most $q^d - 1$ many pairs $(b_i, b_j)$ fulfilling this equation. Thus,

$$\dim(C_0 \cap C_h) \leq d \quad \forall h \in \{1, \ldots, q^n - 2\}.$$

Since we chose $d$ minimal, this inequality is actually an equality for some $h$, hence the minimum distance of the code is $2k - 2d$.

The cardinality of the code follows from the fact that $d < k$, which implies that all elements of the orbit are distinct. $\blacksquare$

**Proposition 35.** *In the setting of before, if $d = k$, one gets orbit elements with full intersection which means they are the same vector space.*

1) *Let $D' := D \setminus \{\{a \in D \mid m_D(a) = q^k - 1\}\}$ and $d' := \log_q(\max\{m_{D'}(a) \mid a \in D'\} + 1)$. Then the minimum distance of the code is $2k - 2d'$.*
2) *Let $m$ be the least element of $D$ of multiplicity $q^k - 1$. Then the cardinality of the code is $m - 1$.*

*Proof:*

1) Since the minimum distance of the code is only taken between distinct vector spaces, one has to consider the largest intersection of two elements whose dimension is less than $k$.
2) Since

$$\mathcal{U}P^m = \mathcal{U} \implies \mathcal{U}P^{lm} = \mathcal{U} \quad \forall l \in \mathbb{N}$$

and the elements of $D$ are taken modulo the order of $P$, one has to choose the minimal element of the multiset $\{\{a \in D \mid m_D(a) = q^k - 1\}\}$ for the number of distinct vector spaces in the orbit. $\blacksquare$

Note, that for $q > 2$ it holds that $\{P^i \mid i = 0, \ldots, \text{ord}(P)\} = \mathbb{F}_q[P]$ and thus contains all scalar multiples of each power of $P$. Therefore, there are at most $(q^n - 1)/(q - 1)$ different vector spaces in the orbit and one will always get $d = k$ when applying Theorem 34.

Tables I–III list binary codes found by randomly picking points in the Grassmannian as initial points of the orbit and computing the minimum distance. Since this search was not exhaustive, the blank fields in the tables do not imply that there are no codes for this set of parameters, but that we have not found any.

In the following we will show that spread codes can be constructed as cyclic orbit codes (cf. [30]). For this let $\alpha$ be a primitive element of $\mathbb{F}_{q^n}$ and assume $k | n$ and $c := \frac{q^n-1}{q^k-1}$. Naturally, the subfield $\mathbb{F}_{q^k} \leq \mathbb{F}_{q^n}$ is also an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$. On the other hand, $\mathbb{F}_{q^k} = \{\alpha^{ic} \mid i = 0, \ldots, q^k - 2\} \cup \{0\}$.

**Algorithm 1** Computing cardinality and minimum distance of primitive cyclic orbit codes in $\mathcal{G}_q(k,n)$

---

**Require:** $p(x) \in \mathbb{F}_q[x]$ primitive of degree $n$, $\alpha$ a root of $p(x)$ and $\mathcal{U} = \{0, u_1, ..., u_{q^k-1}\} \in \mathcal{G}_q(k,n)$
  **for** $u_i$ in $\mathcal{U} \setminus \{0\}$ **do**
    store $\bar{u}_i := \log_\alpha(\phi(v))$
  **end for**
  store all differences $\bar{u}_i - \bar{u}_j$ in the difference multiset $D$
  set $c := \max\{m_D(a) \mid a \in D\}$
  **if** $\log_q(c+1) \neq k$ **then**
    **return** $q^n - 1, 2(k - \log_q(c+1))$
  **else**
    set $c' := \max\{m_D(a) \mid a \in D \text{ and } m_D(a) < c\}$
    set $m := \min\{a \in D \mid m_D(a) = c\}$
    **return** $m-1, 2(k - \log_q(c'+1))$
  **end if**

---

| $d(\mathcal{C})$ \\ $n$ | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|
| 2 | 15 | 31 | 63 | 127 | 255 | 511 | 1023 |
| 4 | 5 | - | 21 | - | 85 | - | 341 |

TABLE I
CARDINALITY OF BINARY PRIMITIVE CYCLIC ORBIT CODES FOR $k = 2$.

| $d(\mathcal{C})$ \\ $n$ | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|
| 2 | 63 | 127 | 255 | 511 | 1023 | 2047 | 4095 |
| 4 | 63 | 127 | 255 | 511 | 1023 | 2047 | 4095 |
| 6 | 9 | - | - | 73 | - | - | 585 |

TABLE II
CARDINALITY OF BINARY PRIM. CYCLIC ORBIT CODES FOR $k = 3$.

| $d(\mathcal{C})$ \\ $n$ | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|
| 2 | 255 | 511 | 1023 | 2047 | 4095 |
| 4 | 255 | 511 | 1023 | 2047 | 4095 |
| 6 | - | 511 | 1023 | 2047 | 4095 |
| 8 | 17 | - | - | - | 273 |

TABLE III
CARDINALITY OF BINARY PRIM. CYCLIC ORBIT CODES FOR $k = 4$.

**Lemma 36.** *For every $\beta \in \mathbb{F}_{q^n}$ the set*

$$\beta \cdot \mathbb{F}_{q^k} = \{\beta\alpha^{ic} \mid i = 0, ..., q^k - 2\} \cup \{0\}$$

*defines an $\mathbb{F}_q$-subspace of dimension $k$.*

*Proof:* Since $\mathbb{F}_{q^k}$ is a subspace of dimension $k$ and

$$\varphi_\beta : \ \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$$
$$u \longmapsto \beta u$$

is an $\mathbb{F}_q$-linear isomorphism, it follows that $\varphi_\beta(\mathbb{F}_{q^k}) = \beta \cdot \mathbb{F}_{q^k}$ is an $\mathbb{F}_q$-subspace of dimension $k$. ∎

**Theorem 37.** *The set*

$$\mathcal{S} = \left\{\alpha^i \cdot \mathbb{F}_{q^k} \mid i = 0, \ldots, c-1\right\}$$

*is a spread of $\mathbb{F}_{q^n}$ and thus defines a spread code in $\mathcal{G}_q(k,n)$.*

*Proof:* By a simple counting argument it is enough to show that the subspaces $\alpha^i \cdot \mathbb{F}_{q^k}$ and $\alpha^j \cdot \mathbb{F}_{q^k}$ have only trivial intersection whenever $0 \leq i < j \leq c-1$. For this assume that there are field elements $\beta_i, \beta_j \in \mathbb{F}_{q^k}$, such that

$$v = \alpha^i \beta_i = \alpha^j \beta_j \in \alpha^i \cdot \mathbb{F}_{q^k} \cap \alpha^j \cdot \mathbb{F}_{q^k}.$$

If $v \neq 0$ then $\alpha^{i-j} = \beta_j \beta_i^{-1} \in \mathbb{F}_{q^k}$. But this means $i - j \equiv 0 \mod c$ and $\alpha^i \cdot \mathbb{F}_{q^k} = \alpha^j \cdot \mathbb{F}_{q^k}$, which contradicts the assumption. It follows that $\mathcal{S}$ is a spread. ∎

We now translate this result into a matrix setting. For this let $\phi$ denote the canonical homomorphism as defined in Theorem 32.

**Corollary 38.** *Assume $k|n$. Then there is a subspace $\mathcal{U} \in \mathcal{G}_q(k,n)$ such that the cyclic orbit code obtained by the group action of a a primitive companion matrix is a code*

with minimum distance $2k$ and cardinality $\frac{q^n-1}{q^k-1}$. *Hence this irreducible cyclic orbit code is a spread code.*

*Proof:* In the setting of the previous theorem represent $\mathbb{F}_{q^k} \leq \mathbb{F}_{q^n}$ as the row space of a $k \times n$ matrix $U$ over $\mathbb{F}_q$ and, using the same basis over $\mathbb{F}_q$, represent the primitive element $\alpha$ with its respective companion matrix $P$. Then the orbit code $\mathcal{C} = \mathrm{rs}(U)\langle P \rangle$ has all the desired properties. ∎

**Example 39.** [30] Over the binary field let $p(x) := x^6 + x + 1$ be primitive, $\alpha$ a root of $p(x)$ and $P$ its companion matrix.

1) For the 3-dimensional spread compute $c = \frac{63}{7} = 9$ and construct a basis for the starting point of the orbit:

$$u_1 = \phi^{-1}(\alpha^0) = \phi^{-1}(1) = (100000)$$
$$u_2 = \phi^{-1}(\alpha^c) = \phi^{-1}(\alpha^9) = \phi^{-1}(\alpha^4 + \alpha^3) = (000110)$$
$$u_3 = \phi^{-1}(\alpha^{2c}) = \phi^{-1}(\alpha^{18}) = \phi^{-1}(\alpha^3 + \alpha^2 + \alpha + 1)$$
$$= (111100)$$

The starting point is

$$\mathcal{U} = \mathrm{rs} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

and the orbit of the group generated by $P$ on $\mathcal{U}$ is a spread code.

2) For the 2-dimensional spread compute $c = \frac{63}{3} = 21$ and construct the starting point

$$u_1 = \phi^{-1}(\alpha^0) = \phi^{-1}(1) = (100000)$$
$$u_2 = \phi^{-1}(\alpha^c) = \phi^{-1}(\alpha^{21}) = \phi^{-1}(\alpha^2 + \alpha + 1)$$
$$= (111000)$$

The starting point is

$$\mathcal{U} = \mathrm{rs} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

and the orbit of the group generated by $P$ is a spread code.

*Non-Primitive Generator:* For this subsection let $p(x) \in \mathbb{F}_q[x]$ be irreducible but not primitive, and, as before, $\alpha$ a root of it and $P$ its companion matrix.

**Proposition 40.** *Let $G = \langle P \rangle$ the group generated by $P$. If $\mathcal{U} \in \mathcal{G}_q(k, n)$ such that*

$$v \neq w \implies vG \neq wG \quad \forall v, w \in \mathcal{U},$$

*then $\mathcal{U}G$ is an orbit code with minimum distance $2k$ and cardinality* $\mathrm{ord}(P)$.

*Proof:* The cardinality follows from the fact that each element of $\mathcal{U}$ has its own orbit of cardinality $\mathrm{ord}(P)$. Moreover, no code words intersect non-trivially, hence the minimum distance is $2k$. ∎

Note that, if the order of $P$ is equal to $\frac{q^n-1}{q^k-1}$, these codes are again spread codes.

**Example 41.** Over the binary field let $p(x) = x^4 + x^3 + x^2 + x + 1$, $\alpha$ a root of $p(x)$ and $P$ its companion matrix. Then $\mathbb{F}_{2^4} \setminus \{0\}$ is partitioned into

$$\{\alpha^i | i = 0, \ldots, 4\} \cup \{\alpha^i(\alpha + 1) | i = 0, \ldots, 4\}$$

$$\cup \{\alpha^i(\alpha^2 + 1) | i = 0, \ldots, 4\}.$$

Choose

$$u_1 = \phi^{-1}(1) = \phi^{-1}(\alpha^0) = (1000)$$
$$u_2 = \phi^{-1}(\alpha^3 + \alpha^2) = \phi^{-1}(\alpha^2(\alpha + 1)) = (0011)$$
$$u_3 = u_1 + u_2 = \phi^{-1}(\alpha^3 + \alpha^2 + 1) = \phi^{-1}(\alpha^4(\alpha^2 + 1))$$
$$= (1011)$$

such that each $u_i$ is in a different orbit of $\langle P \rangle$ and $\mathcal{U} = \{0, u_1, u_2, u_3\}$ is a vector space. Then the orbit of $\langle P \rangle$ on $\mathcal{U}$ has minimum distance $4$ and cardinality $5$, hence it is a spread code.

The following theorem generalizes this result to any possible starting point in $\mathcal{G}_q(k, n)$ and can be proven analogously to Theorem 34.

**Theorem 42.** *[30] Let $P, G, \mathcal{U}$ be as before and $O_1, ..., O_\ell$ the distinct orbits of $G$ on $\mathbb{F}_q^n \setminus \{0\}$. Assume that $m_i$ elements of $\mathcal{U}$ are in the same orbit $O_i$ $(i = 1, \ldots, \ell)$. Apply the theory of Section V-A to each orbit $O_i$ and find the corresponding $d_i$ from Theorem 34. Then the following cases can occur:*

1) *No intersections of two different orbits coincide. Define $d := \max_i d_i$. Then the orbit of $G$ on $\mathcal{U}$ is a code of cardinality $\mathrm{ord}(P)$ and minimum distance $2k - 2d$.*

2) *Some intersections coincide among some orbits. Then the corresponding $d_i$'s add up and the maximum of these is the maximal intersection number $d$.*

*Mathematically formulated: Assume the orbits are of the type*

$$O_i = \{\tilde{p}_i(\alpha)\alpha^j \mid j = 1, \ldots, \mathrm{ord}(P)\} \quad \forall i = 1, \ldots, \ell$$

*for some fixed $\tilde{p}_i(\alpha) \in \mathbb{F}_q[\alpha]$. Then for any $u_j \in O_i$ there exists $b_{(i,j)} \in \mathbb{Z}_{\mathrm{ord}(P)}$ such that*

$$\phi(u_j) = \tilde{p}_i(\alpha)\alpha^{b_{(i,j)}}.$$

*For $i = 1, \ldots, \ell$ define*

$$a_{(i,\mu,\lambda)} := b_{(i,\mu)} - b_{(i,\lambda)}$$

*and the difference multisets*

$$D_i := \{\{a_{(i,\mu,\lambda)} \mid \mu, \lambda \in \{1, \ldots, \mathrm{ord}(P) - 1\}\}\},$$

$$D := \bigcup_{i=1}^{\ell} D_i.$$

*Let $d := \log_q(\max\{m_D(a) \mid a \in D\} + 1)$. If $d < k$, then the orbit of $G$ on $\mathcal{U}$ is a code of cardinality $\mathrm{ord}(P)$ and minimum distance $2k - 2d$.*

If $d = k$, Proposition 35 also holds in this (non-primitive) case. The algorithm works analogously to Algorithm 1.

Tables IV–VI list binary cyclic orbit codes generated by irreducible polynomials of degree 10 with different orders, found by random search. By "X" we denote a set of parameters that cannot be fulfilled. As before, a "−" means that we have not found a code for these parameters and not neccessarily that there do not exist any.

| $d(\mathcal{C})$ \ $k$ | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| 2 | 33 | 33 | 33 | 33 |
| 4 | 33 | 33 | 33 | 33 |
| 6 | X | 33 | 33 | 33 |
| 8 | X | X | - | 33 |
| 10 | X | X | X | - |

TABLE IV
CARDINALITY OF CODES GENERATED BY A POLYNOMIAL OF ORDER 33 FOR $n = 10$.

| $d(\mathcal{C})$ \ $k$ | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| 2 | 93 | 93 | 93 | 93 |
| 4 | 93 | 93 | 93 | 93 |
| 6 | X | 93 | 93 | 93 |
| 8 | X | X | - | - |
| 10 | X | X | X | - |

TABLE V
CARDINALITY OF CODES GENERATED BY A POLYNOMIAL OF ORDER 93 FOR $n = 10$.

| $d(\mathcal{C})$ \ $k$ | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| 2 | 341 | 341 | 341 | 341 |
| 4 | 341 | 341 | 341 | 341 |
| 6 | X | - | 341 | 341 |
| 8 | X | X | - | - |
| 10 | X | X | X | - |

TABLE VI
CARDINALITY OF CODES GENERATED BY A POLYNOMIAL OF ORDER 341 FOR $n = 10$.

## B. Completely reducible cyclic orbit codes

We call an orbit code completely reducible if its generating group is completely reducible. In general, a group is *completely reducible* or *semisimple* if it is the direct product of irreducible groups. For the $\mathrm{GL}_n$-action on $\mathbb{F}_q^n$ a subgroup $H \leq \mathrm{GL}_n$ is completely reducible if $\mathbb{F}_q^n$ is the direct sum of subspaces $V_1, \ldots, V_i$ which are $H$-invariant but do not have any $H$-invariant proper subspaces.

In the cyclic case these groups are exactly the ones where the blocks of the rational canonical form of the generator matrix are companion matrices of irreducible polynomials, i.e. all the elementary divisors have exponent 1. Because of this property one can use the theory of irreducible cyclic orbit codes block-wise to compute the minimum distances of the block component codes and hence the minimum distance of the whole code.

For simplicity we will explain how the theory from before generalizes in the case of generator matrices whose RCF has two blocks that are companion matrices of primitive polynomials. The generalization to an arbitrary number of blocks and general irreducible polynomials is then straightforward.

Assume our generator matrix $P$ is of the type

$$P = \begin{pmatrix} P_1 & 0 \\ 0 & P_2 \end{pmatrix}$$

where $P_1, P_2$ are companion matrices of the primitive polynomials $p_1(x), p_2(x) \in \mathbb{F}_q[x]$ with $\deg(p_1) = n_1, \deg(p_2) = n_2$, respectively. Furthermore let

$$U = \begin{bmatrix} U_1 & U_2 \end{bmatrix}$$

be the matrix representation of the starting point $\mathcal{U} \in \mathcal{G}_q(k, n)$ such that $U_1 \in Mat_{k \times n_1}, U_2 \in Mat_{k \times n_2}$. Then

$$\mathcal{U}P^i = \mathrm{rs} \begin{bmatrix} U_1 P_1^i & U_2 P_2^i \end{bmatrix}.$$

By $\phi^{(n_1)} : \mathbb{F}_q^{n_1} \to \mathbb{F}_{q^{n_1}}$ and $\phi^{(n_2)} : \mathbb{F}_q^{n_2} \to \mathbb{F}_{q^{n_2}}$ we denote the standard vector space isomorphisms.

The algorithm for computing the minimum distance of the orbit code is analogous to before, but it is now set in $\mathbb{F}_{q^{n_1}} \times \mathbb{F}_{q^{n_2}}$.

**Theorem 43.** *Let $\alpha_1, \alpha_2$ be primitive elements of $\mathbb{F}_{q^{n_1}}, \mathbb{F}_{q^{n_2}}$ respectively.*

$$\phi^{(n_1,n_2)} : \mathbb{F}_q^n \longrightarrow \mathbb{F}_{q^{n_1}} \times \mathbb{F}_{q^{n_2}}$$
$$(u_1, ..., u_n) \longmapsto (\phi^{(n_1)}(u_1, ..., u_{n_1}), \phi^{(n_2)}(u_{n_1+1}, ..., u_n))$$

*is a vector space isomorphism. Moreover, $u = vP^i$ for some $u, v \in \mathbb{F}_q^n$ if and only if*

1) $\phi^{(n_1)}(u_1, ..., u_{n_1}) = \phi^{(n_1)}(v_1, ..., v_{n_1})\alpha_1^i$ *and*
2) $\phi^{(n_2)}(u_{n_1+1}, ..., u_n) = \phi^{(n_2)}(v_{n_1+1}, ..., v_n)\alpha_2^i$.

*Proof:* $\phi^{(n_1,n_2)}$ is a vector space isomorphism because $\phi^{(n_1)}$ and $\phi^{(n_2)}$ are. The second statement follows since

$$u = vP^i$$
$$\iff \phi^{(n_1,n_2)}(u) = \phi^{(n_1,n_2)}(vP^i)$$
$$\iff \phi^{(n_1)}((u_1, ..., u_{n_1})) = \phi^{(n_1)}((v_1, ..., v_{n_1})P_1^i) \wedge$$
$$\phi^{(n_2)}((u_{n_1+1}, ..., u_n)) = \phi^{(n_2)}((v_{n_1+1}, ..., v_n)P_2^i).$$

Thus, if $\phi^{(n_1)}(u_i) \neq 0$ and $\phi^{(n_2)}(u_i) \neq 0$ for all non-zero elements $u_i$ of a given vector space $\mathcal{U} \in \mathcal{G}_q(k, n)$, in the algorithm we have to create the difference set of all 2-tuples corresponding to the powers of $\alpha_1$ and $\alpha_2$ and proceed as usual.

**Proposition 44.** *Assume $\mathcal{U} = \{0, u_1, \ldots, u_{q^k-1}\} \in \mathcal{G}_q(k, n)$, and for all $u_i$ there exist $b_i, b_i'$ such that*

$$\phi^{(n_1,n_2)}(u_i) = (\alpha_1^{b_i}, \alpha_2^{b_i'}) \qquad \forall i = 1, \ldots, q^k - 1.$$

*Let $d$ be minimal such that any element of the multiset*

$$D := \{\{(b_m - b_\ell \mod q^{n_1} - 1, b_m' - b_\ell' \mod q^{n_2} - 1) \mid$$
$$\ell, m \in \mathbb{Z}_{q^k-1}, \ell \neq m\}\}$$

*has multiplicity less than or equal to $q^d - 1$. If $d < k$ then the orbit of the group generated by $P$ on $\mathcal{U}$ is an orbit code of cardinality $\mathrm{ord}(P) = \mathrm{lcm}(q^{n_1} - 1, q^{n_2} - 1)$ and minimum distance $2k - 2d$.*

Since it is possible that $u = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$ is non-zero but all $u_1 = \cdots = u_{n_1} = 0$ (or the second part of the coefficients), we have to take the zero element into account when counting intersection elements:

**Theorem 45.** *Assume $\mathcal{U} = \{0, u_1, \ldots, u_{q^k-1}\} \in \mathcal{G}_q(k, n)$, and for all $u_i$ either*

1) $\phi^{(n_1,n_2)}(u_i) = (\alpha_1^{b_i}, \alpha_2^{b_i'})$,
2) $\phi^{(n_1,n_2)}(u_i) = (\alpha_1^{b_i}, 0)$ *or*
3) $\phi^{(n_1,n_2)}(u_i) = (0, \alpha_2^{b_i'})$.

*Denote by $S_1, S_2, S_3$ the sets of all elements of the first, second and third type, respectively, and construct the difference sets*

$$D_1 := \{\{(b_m - b_\ell \mod q^{n_1} - 1, b_m' - b_\ell' \mod q^{n_2} - 1) \mid$$
$$u_\ell, u_m \in S_1, \ell \neq m\}\},$$
$$D_2 := \{\{(b_m - b_\ell \mod q^{n_1} - 1, j) \mid u_\ell, u_m \in S_2, \ell \neq m,$$
$$j = 1, \ldots, q^{n_2} - 1\}\},$$
$$D_3 := \{\{(j, b_m' - b_\ell' \mod q^{n_2} - 1) \mid u_\ell, u_m \in S_3, \ell \neq m,$$
$$j = 1, \ldots, q^{n_1} - 1\}\}$$

*and*

$$D := D_1 \cup D_2 \cup D_3.$$

*Let $d$ be minimal such that any element of $D$ has multiplicity less than or equal to $q^d - 1$. If $d < k$ then the orbit of the group generated by $P$ on $\mathcal{U}$ is an orbit code of cardinality $\mathrm{ord}(P) = \mathrm{lcm}(q^{n_1}-1, q^{n_2}-1)$ and minimum distance $2k-2d$.*

*Proof:* As in the irreducible case we want to count the number of intersecting elements and use the fact that $\langle P_1 \rangle, \langle P_2 \rangle$ act transitively on $\mathbb{F}_q^{n_1} \setminus \{0\}$ and $\mathbb{F}_q^{n_2} \setminus \{0\}$ respectively. Let $\pi_1 : \mathbb{F}_q^n \to \mathbb{F}_q^{n_1}, (u_1, \ldots, u_n) \mapsto (u_1, \ldots, u_{n_1})$ and $\pi_2 : \mathbb{F}_q^n \to \mathbb{F}_q^{n_2}, (u_1, \ldots, u_n) \mapsto (u_{n_1+1}, \ldots, u_{n_2})$.

1) Assume $u \in S_3$, i.e. $\pi_1(u) = 0$. Then

$$\pi_1(uP^i) = \pi_1(u)P_1^i = 0 \quad \forall i = 1, \ldots, \mathrm{ord}(P).$$

Thus, $uP^j \neq v$ for all $v \in S_1 \cup S_2$ and $j = 1, \ldots, \mathrm{ord}(P)$, i.e. intersection with $u$ can only happen inside $S_3$.

On the other hand, if $\pi_2(u) = \pi_2(u)P_2^j$ for some $j$, then also $u = uP^j$, which is why the second entry of the tuple can run over all possible values.

2) For $u \in S_2$ the analogue holds.

3) For $u \in S_1$ we can use Proposition 44.

Since we have to check if some of the intersections inside the sets $S_1, S_2, S_3$ occur at the same element of the orbit we have to count the intersection inside the union of the difference sets. ∎

Like in the irreducible case, if $d = k$, one gets orbit elements with full intersection. Let $D' := D \setminus \{\{a = (a_1, a_2) \in D \mid m_D(a) = q^k - 1\}\}$ and $d' := \log_q(\max\{m_{D'}(a) \mid a \in D'\} + 1)$. Then the minimum distance of the code is $2k - 2d'$. Moreover, let $m := \min\{\text{lcm}(a_1, a_2) \mid a = (a_1, a_2) \in D, m_D(a) = q^k - 1\}$. Then the cardinality of the code is $m - 1$.

### C. Non- completely reducible cyclic orbit codes

If a matrix has elementary divisors of exponent larger than one, the group generated by it is not completely reducible. In this subsection we will explain what happens in this case when you try to apply the theory from the previous subsections. For simplicity we will describe the case of polynomials that are squares of an irreducible one. This can easily be generalized to higher exponents. Along the lines of the previous subsection one can then translate the theory to more than one irreducible factor block-wise.

Let $p(x) \in \mathbb{F}_q[x]$ be irreducible of degree $n/2$ and $f(x) = p^2(x)$. Denote by $P_f$ the companion matrix of $f(x)$. Since a root of $f(x)$ is also a root of $p(x)$ we can not use it to represent $\mathbb{F}_q[x]_{<n} \cong \mathbb{F}_q^n$. Therefore we will now use polynomials in the variable $x$ and the standard vector space isomorphism $\phi : \mathbb{F}_q^n \to \mathbb{F}_q[x]_{<n}, (u_1, \ldots, u_n) \mapsto \sum_{i=1}^n u_i x^{i-1}$. Then the following still holds:

$$\phi(uP_f) = \phi(u)x \mod f(x).$$

Hence, one can still translate the question of finding the intersection number into the polynomial setting by finding the respective $x^i$ that maps one element to another element of the initial point $\mathcal{U} \in \mathcal{G}_q(k, n)$. The difference to the cases before is that we do not have a field structure anymore, thus in general we cannot divide one element by the other modulo $f(x)$ to find the corresponding $x^i$. More precisely, we can divide by the units of $\mathbb{F}_q[x]/(f(x))$. In the other cases we can find the $x^i$ by brute force.

**Theorem 46.** *Assume* $\mathcal{U} = \{0, u_1, \ldots, u_{q^k-1}\} \in \mathcal{G}_q(k, n)$,

$$\phi(u_i) = \phi(u_j)x^{b_{ij}}$$

*for all* $\phi(u_i), \phi(u_j)$ *that lie on the same orbit of* $\langle x \rangle$ *and* $d$ *be minimal such that any element of the multiset*

$$D := \{\{b_{ij} \mod q^n - 1 \mid i, j \in \mathbb{Z}_{q^k-1}, i \neq j\}\}$$

*has multiplicity less than or equal to* $q^d - 1$. *If* $d < k$ *then the orbit of the group generated by* $P_f$ *on* $\mathcal{U}$ *is an orbit code of cardinality* $q^{\frac{n}{2}} - 1$ *and minimum distance* $2k - 2d$.

## VI. DECODING PRIMITIVE CYCLIC ORBIT CODES

In this section we will show how to decode primitive cyclic orbit codes. Let $\mathcal{U} \in \mathcal{G}_q(k, n)$, $\alpha \in \mathbb{F}_q^n$ a primitive element, $P \in \text{GL}_n$ the corresponding companion matrix, $G = \langle P \rangle$ and $\mathcal{C} = \mathcal{U}G$ the generated orbit code with minimum distance $2\delta$.

If $\mathcal{V} \in \mathcal{C}$ denotes the sent code word and $\mathcal{R} \in \mathcal{P}_q(n)$ the received vector space, then $\mathcal{R}$ is uniquely decodable if $d(\mathcal{R}, \mathcal{V}) \leq \delta - 1$.

A minimum distance decoder finds $A \in G$, such that

$$d(\mathcal{R}, \mathcal{U}A) \leq d(\mathcal{R}, \mathcal{U}A')$$

$$\iff \dim(\mathcal{R} \cap \mathcal{U}A) \geq \dim(\mathcal{R} \cap \mathcal{U}A')$$

for all $A' \in G$. If $\mathcal{R}$ is decodable then it holds that

$$d(\mathcal{R}, \mathcal{U}A) < d(\mathcal{R}, \mathcal{U}A')$$

for all $A' \in G \setminus \text{Stab}_G(\mathcal{U}A)$.

We will now explain how the canonizer mapping, explained in Section III-B, can efficiently be computed for primitive cyclic orbit codes.

**Lemma 47.** *Let* $\mathcal{U}, \mathcal{V} \in \mathcal{P}_q(n)$ *be non-trivial. Then there exists* $A \in G$ *such that* $\dim(\mathcal{U} \cap \mathcal{V}A) \geq 1$.

*Proof:* Follows directly from the transitivity of $G$. ∎

**Lemma 48.** *Let* $\mathcal{U}, \mathcal{V} \in \mathcal{P}_q(n)$ *and* $P^i \in G$ *with* $\dim(\mathcal{U} \cap \mathcal{V}P^i) \geq 1$. *Then there exist* $u \in \mathcal{U}$ *and* $v \in \mathcal{V}$ *such that* $\phi(u)\phi(v)^{-1} \equiv \alpha^i \mod q^n - 1$.

*Proof:* Since $\dim(\mathcal{U} \cap \mathcal{V}P^i) \geq 1$, there is a non-zero vector $u \in \mathcal{U} \cap \mathcal{V}P^i$. Then there exists a vector $v \in \mathcal{V} - \{0\}$ with $u = vP^i$. Hence, in field representation it holds that $\phi(u)\phi(v)^{-1} \equiv \alpha^i \mod q^n - 1$. ∎

This leads to the following algorithm, for which we first need to define yet another vector space isomorphism:

$$\psi : \quad G \longrightarrow \mathbb{F}_{q^n}$$

$$\sum_{i=0}^{n-1} \lambda_i P^i \longmapsto \sum_{i=0}^{n-1} \lambda_i \alpha^i$$

where $\lambda_i \in \mathbb{F}_q$.

---

**Algorithm 2** Minimum distance decoder for primitive cyclic orbit codes in $\mathcal{G}_q(k, n)$.

---

**Require:** Code $\mathcal{C} = \mathcal{U}\langle P \rangle \subseteq \mathcal{G}_q(k, n)$, received word $\mathcal{R} \in \mathcal{P}_q(n)$

  set $d := 0, g := 0$
  **for** $v \in \mathcal{R} \setminus \{0\}$ **do**
    **for** $u \in \mathcal{U} \setminus \{0\}$ **do**
      compute $g' := \phi(v)\phi(u)^{-1}$ in $\mathbb{F}_{q^n}$
      compute $d' := \dim(\mathcal{R} \cap \mathcal{U}\psi^{-1}(g'))$
      **if** $d' > d$ **then**
        set $d := d'$ and $g := g'$
      **end if**
    **end for**
  **end for**
  **return** $\mathcal{U}\psi^{-1}(g')$

**Theorem 49.** *If* $\dim(\mathcal{R}) := k'$*, the complexity of Algorithm 2 is* $\mathcal{O}(q^{k+k'}(n^2 + (k+k')^2 n))$ *over* $\mathbb{F}_q$.

*Proof:*

1) In order to the determine the group element $g'$ one division in the finite field $\mathbb{F}_{q^n}$ must be performed which has complexity $\mathcal{O}(n^2)$.
2) We compute the dimension of the intersection of subspaces with the aid of the Gaussian algorithm. Since $\dim(\mathcal{U}) = k$ and $\dim(\mathcal{R}) = k'$, the complexity is given by $\mathcal{O}((k+k')^2 n)$.
3) The complexity of the algorithm is mainly determined by the two nested loops, i. e. the inner steps from above must be performed $(q^{\dim(\mathcal{U})} - 1)(q^{\dim(\mathcal{R})} - 1)$ times. ∎

We can improve the complexity by choosing only specific elements of the received space to compute with in the algorithm. For this we need the following theorem.

**Theorem 50.** *[24] Let* $v_1, \ldots, v_k \in \mathbb{F}_q^n$ *be a basis of the sent code word* $\mathcal{V} \in \mathcal{G}_q(k, n)$ *and* $r_1, \ldots, r_{k'} \in \mathbb{F}_q^n$ *a basis of the received space* $\mathcal{R}$*. Assume* $f < k'$ *linearly independent error vectors were inserted during transmission, i.e.* $\mathcal{R} = \mathcal{V}' \oplus \mathcal{E}$*, where* $\mathcal{V}'$ *is a vector subspace of* $\mathcal{V}$ *and* $\mathcal{E}$ *is the vector space spanned by the error vectors. Then the set*

$$\mathcal{L}_f := \left\{ \sum_{i \in I} \lambda_i r_i \mid \lambda_i \in \mathbb{F}_q, I \in \binom{[k']}{f} \right\}$$

*contains* $k' - f$ *linearly independent elements of* $\mathcal{V}$*. By* $\binom{[k']}{f}$ *we denote the set of all subsets of* $\{1, 2, \ldots, k'\}$ *of size* $f$.

*Proof:* Inductively on $f$:

1) If $f = 0$, then $r_1, \ldots, r_{k'} \in \mathcal{U}$.
2) If $f = 1$, assume $r_1, \ldots, r_\ell \in \mathcal{E}$ and $r_{\ell+1}, \ldots, r_{k'} \in \mathcal{U}'$. Then

$$r_i = \sum_{j=1}^{k} \lambda_{ij} v_j + \mu_i e \quad \forall i = 1, \ldots, l$$

where $e \in \mathcal{E}$ denotes the error vector, and hence $\forall i, h = 1, \ldots, l$

$$r_i + r_h = \sum_{j=1}^{k} (\lambda_{ij} + \lambda_{hj}) v_j + (\mu_i + \mu_h) e$$

$$\implies r_i + (-\mu_i \mu_h^{-1}) r_h = \sum_{j=1}^{k} (\lambda_{ij} + \lambda_{hj}) v_j.$$

Then the elements $r_{\ell+1}, \ldots, r_{k'}, r_1 + (-\mu_1 \mu_2^{-1}) r_2, \ldots, r_1 + (-\mu_1 \mu_\ell^{-1}) r_\ell$ are $k' - 1$ linearly independent elements without errors.
3) If more errors, say $e_1, \ldots, e_f$, were inserted, then one can inductively "erase" $f - 1$ errors in the linear combinations of at most $f$ elements. Write the received elements as

$$r_i = \sum_{j=1}^{k} \lambda_{ij} v_j + \sum_{j=1}^{f} \mu_{ij} e_j \quad \forall i = 1, \ldots, k'.$$

Assume $\mu_{1f}, \ldots, \mu_{\ell f} \neq 0$ and $\mu_{(l+1)f}, \ldots, \mu_{k'f} = 0$, i.e. the first $l$ elements involve $e_f$ and the others do not. From above we know that the linear combinations of any two elements of $r_1, \ldots, r_\ell$ will include $l - 1$ linearly independent elements without $e_f$. Denote them by $m_1, \ldots, m_{\ell-1}$. Naturally these elements are also linearly independent from $r_{\ell+1}, \ldots, r_{k'}$. Use the induction step on $m_1, \ldots, m_{\ell-1}, r_{\ell+1}, \ldots, r_{k'}$ to get $k' - 1 - (f-1) = k' - f$ linearly independent elements without errors. ∎

Hence, if the received word is decodable, the set $\mathcal{L}_f$ contains at least one element $v$ of the sent word $\mathcal{V}$. For this element it holds that there exists $u \in \mathcal{U} \setminus \{0\}$ such that

$$\dim(\mathcal{R} \cap \mathcal{U}\psi^{-1}(\phi(v)\phi(u)^{-1})) \geq k + k' - \delta + 1$$

$$\iff d(\mathcal{R}, \mathcal{U}\psi^{-1}(\phi(v)\phi(u)^{-1})) \leq \delta - 1.$$

Therefore, Algorithm 2 is improved by replacing the outer FOR-loop "**for** $v \in \mathcal{R} \setminus \{0\}$ **do**" by "**for** $v \in \mathcal{L}_f \setminus \{0\}$ **do**".

If the number $f$ of inserted errors is unknown, one can set $f$ equal to the error-correction capability of the code. Since $d(\mathcal{R}, \mathcal{V}) \leq \delta - 1$, the error-correction capability is equal to

$$\dim(\mathcal{E}) = k' - \dim(\mathcal{R} \cap \mathcal{V})$$
$$\leq k' - \frac{1}{2}(k' + k - \delta + 1)$$
$$= \frac{1}{2}(k' - k + \delta - 1).$$

More efficiently, the algorithm can iteratively work over $\mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_f$ and return the respective result as soon as $d' \geq k + k' - \delta + 1$ is found.

The complexity of the improved algorithm differs from the one before only in the number of loops. Instead of $q^{k'} - 1$ we now have $\sum_{i=1}^{f+1} \binom{k'}{i}(q-1)^i$ elements of $\mathcal{R}$ to check.

Figures 2 and 3 compare the numbers $q^k - 1$ (red graph) and $\sum_{i=1}^{f+1} \binom{k}{i}(q-1)^i$ (blue graph) for different values of $q$ and $f$ and thus depict that for increasing $q$ and small $f$ the complexity is greatly improved.
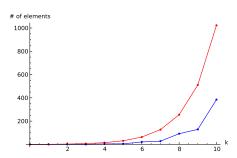


Fig. 2. $q = 2, f = \lfloor k/2 \rfloor$-2

In comparison, the decoding algorithms for Reed-Solomon like codes contained in [18] and [25] in the case of $k = k'$ have a complexity of $\mathcal{O}(n^2(n-k)^2)$ and $\mathcal{O}(\delta(n-k)^3)$, respectively.

In [12] the authors present a minimum distance decoder for their spread code construction. The complexity of their algorithm is $\mathcal{O}((n - k)k^3)$. Another spread decoder is presented in [24], whose complexity is $\mathcal{O}(nk(qk)^{f+1})$.
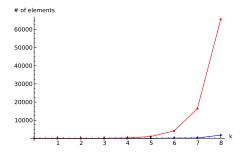
Fig. 3. $q = 4, f = \lfloor k/2 \rfloor\text{-}2$

**Remark 51.** *The presented algorithm also works for non-primitive irreducible cyclic orbit codes. The only main difference is that $G$ is not transitive and thus Lemma 47 does not hold for arbitrary elements. Nonetheless the subsequent results are still correct if one assumes that the received space $\mathcal{R}$ is decodable. Moreover, in Lemma 47 "$\alpha^i$" has to be changed to an element from $\mathbb{F}_q[\alpha]$.*

## VII. CONCLUSIONS

In the first part we presented an overview of orbit codes in general and showed how these are a natural generalization of the concept of linearity for block codes. The main results of this part are that the minimum distance of the whole code is equal to the minimal distance between the initial point and any other point on the orbit and that one can define syndrome-like decoding for these codes.

Furthermore, we investigated cyclic orbit codes in the Grassmannian in more detail. For that we first showed how to classify them by the rational canonical forms of their generators. Then we showed how to compute the minimum distance of cyclic orbit codes and gave some examples of cardinalites and minimum distances found by random search. Moreover, we showed that spread codes can be constructed as primitive cyclic orbit codes for any set of valid parameters. In the end we explained how to decode irreducible cyclic orbit codes and determined the complexity of the proposed algorithm, which is efficient if the field size $q$ and the dimension of the vector spaces $k$ is small.

For further research it would be natural to generalize our presented results to arbitrary groups with more than one generator. Another interesting question is whether there are subgroups of the general linear group where the canonizing mapping is easily computed. For these groups an efficient minimum distance decoder can easily be derived. Furthermore, it is an open question what an encoder map from the actual message space could be.

Although one loses some of the algebraic structure it is still an interesting project to investigate unions of orbit codes. In the primitive case some research in this area has already been done in [17], but the more general case is unknown. Moreover, it is interesting to see what combinations of orbits will keep some algebraic structure and how this can be exploited for decoding.

## REFERENCES

[1] R. Ahlswede, N. Cai, S.-Y.R. Li, and R.W. Yeung. Network Information Flow. *IEEE Transactions on Information Theory*, 46:1204–1216, 2000.
[2] E. Artin. *Geometric Algebra*. Interscience Publishers, Inc., New York, 1957.
[3] R. Baer. *Linear Algebra and Projective Geometry*. Academic Press, New York, 1952.
[4] G. Birkhoff. *Lattice Theory*. American Mathematical Society, third edition, 1967.
[5] M. Braun. Lattices, Binary Codes, and Network Codes. *Advances in the Mathematics of Communications, Special Issue on Algebraic Combinatorics and Applications, April 11-18, 2010, Thurnau, Germany — ALCOMA'10*, 5(2):225–232, 2011.
[6] M. Braun, T. Etzion, and A. Vardy. Linearity and Complements in Projective Space. *arXiv:1103.3117v1*, [cs.IT], 2011.
[7] J. D. Dixon and B. Mortimer. *Permutation Groups*. Springer-Verlag, 1996.
[8] A. Elsenhans, A. Kohnert, and Alfred Wassermann. Construction of Codes for Network Coding. In *Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems — MTNS'10*, pages 1811–1814, Budapest, Hungary, 2010.
[9] T. Etzion and N. Silberstein. Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams. *IEEE Transactions on Information Theory*, 55(7):2909–2919, 2009.
[10] T. Etzion and A. Vardy. Coding Theory in Projective Spaces. In *Information Theory and Applications Workshop, 2008, Jan. 27th - Feb. 1st*, San Diego, USA, 2008.
[11] T. Etzion and A. Vardy. Error-Correcting Codes in Projective Space. In *IEEE International Symposium on Information Theory, 2008 — ISIT 2008*, pages 871–875, 2008.
[12] E. Gorla, F. Manganiello and J. Rosenthal. An Algebraic Approach for Decoding Spread Codes. *arXiv:1107.55237v1*, [cs.IT], 2011.
[13] I. N. Herstein. *Topics in algebra*. 2nd ed. Lexington, Mass.: Xerox College Publishing, 1975.
[14] J. W. P. Hirschfeld. *Projective Geometries over Finite Fields*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second edition, 1998.
[15] A. Kerber. *Applied Finite Group Actions*. Springer-Verlag, 1999.
[16] A. Khaleghi, D. Silva, and F. R. Kschischang. Subspace Codes. In *Proceedings of the 12th IMA International Conference on Cryptography and Coding*, Cryptography and Coding '09, pages 1–21. Springer-Verlag, 2009.
[17] A. Kohnert and S. Kurz. Construction of Large Constant Dimension Codes with a Prescribed Minimum Distance. In Jacques Calmet, Willi Geiselmann, and Jörn Müller-Quade, editors, *MMICS*, volume 5393 of *Lecture Notes in Computer Science*, pages 31–42. Springer, 2008.
[18] R. Kötter and F. R. Kschischang. Coding for Errors and Erasures in Random Network Coding. *IEEE Transactions on Information Theory*, 54(8):3579–3591, 2008.
[19] E. Kramer and D. Mesner. *t*-Designs on Hypergraphs. *Discrete Mathematics*, 15(3):263–296, 1976.
[20] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and their Applications*. Cambridge University Press, Cambridge, London, 1986.
[21] J. H. van Lint and R. M. Wilson. *A Course in Combinatorics*. Cambridge University Press, second edition, 2001.
[22] F. Manganiello, E. Gorla, and J. Rosenthal. Spread Codes and Spread Decoding in Network Coding. In *Proceedings of the 2008 IEEE International Symposium on Information Theory (ISIT)*, pages 851–855, 6-11 July 2008.
[23] F. Manganiello, A.-L. Trautmann, and J. Rosenthal. On Conjugacy Classes of Subgroups of the General Linear Group and Cyclic Orbit Codes. In *Proceedings of the 2011 IEEE International Symposium on Information Theory (ISIT)*, pages 1916–1920, July 31 2011-Aug. 5 2011.
[24] F. Manganiello and A.-L. Trautmann. Spread Decoding in Extension Fields. *arXiv:1108.5881v1*, [cs.IT], 2011.
[25] D. Silva, F. R. Kschischang, and R. Kötter. A Rank-Metric Approach to Error Control in Random Network Coding. *IEEE Transactions on Information Theory*, 54(9):3951–3967, 2008.
[26] V. Skachek. Recursive Code Construction for Random Networks. *IEEE Transactions on Information Theory*, 56(3):1378–1382, 2010

[27] D. Slepian. Group Codes for the Gaussian Channel. *Bell System Technical Journal*, 47:575–602, 1968.

[28] S. Thomas. Designs over Finite Fields. *Geometriae Dedicata*, 24:237–242, 1987.

[29] A.-L. Trautmann, F. Manganiello, and J. Rosenthal. Orbit Codes—A new Concept in the Area of Network Coding. In *IEEE Information Theory Workshop, Dublin, Ireland, August 2010 — ITW 2010*, pages 1–4, 2010.

[30] A.-L. Trautmann and J. Rosenthal. A Complete Characterization of Irreducible Cyclic Orbit Codes. In *Proceedings of the Seventh International Workshop on Coding and Cryptography — WCC 2011*, pages 219–223, 2011.